Integrating Failure Detection and Isolation into a Reference Governor-Based Reconfiguration Strategy for Stuck Actuators

Huayi Li, Ilya Kolmanovsky, and Anouck Girard

***Abstract*— A set-theoretic Failure Model and Effect Management (FMEM) strategy for stuck/jammed actuators in systems with redundant actuators is considered. This strategy uses a reference governor for command tracking while satisfying state and control constraints and, once the failure mode is known, generates a recovery command sequence during mode transitions triggered by actuator failures. In the paper, this FMEM strategy is enhanced with a scheme to detect and isolate failures within a finite time, and to handle unmeasured set-bounded disturbance inputs. A numerical example is reported to illustrate the offline design process and the online operation with the proposed approach.**

I. INTRODUCTION

Stuck/jammed actuators, unless properly handled by a Failure Mode and Effect Management (FMEM) system, can result in a marked degradation of system performance and safety, with notable examples such as [1]. Systems that are highly automated and designed to fulfill complex missions often exploit actuator redundancy and comprehensive fault-tolerant control (FTC) schemes to ensure reliability and safety. To handle the multitude of potential failure modes, a systematic development process of such FMEM strategies that is capable of handling sequential failures and has guaranteed properties by design is highly desirable.

In this paper, we develop several enhancements to a reference governor-based set-theoretic FMEM strategy that was introduced in our previous work [2]. This strategy handles stuck/jammed actuators while tracking reference commands. It relies on the reference governor for operating the system subject to constraints in different operating modes and generates a recovery reference command sequence once failure is detected to effect the transition into the new operating mode with a different number of functioning actuators. The proposed enhancements include the integration of a scheme that detects and isolates failures in finite time before the recovery command sequence is generated, thereby relaxing the negligibly small time assumption for failure detection and isolation (FDI) in [2]. Additionally, set-bounded unmeasured disturbance inputs are handled.

The literature on FDI and failure mode reconfiguration is extensive, see e.g., [3], [4]; however, reference command tracking in presence of state and control constraints is often not the focus and the design of the system to handle sequential failures is frequently not considered. In the reference command tracking setting, several reference governor-based approaches have been proposed such as in [5], [6] and references therein, with the approach closest to ours being [5]. A notable difference is that in our work, [2], [7] and this paper, we pursue a deterministic treatment (based on set-theoretic control) that leads to a possibility of FDI and failure mode reconfiguration in finite time rather than asymptotically in a probabilistic sense, while guaranteeing that the constraints are enforced in all operation phases. Other approaches utilizing set-theoretic methods in systems with failures are proposed in, e.g., [8], [9].

Fault detection and diagnosis, isolation, identification, and reconfiguration are essential components of active FTC [10] but they are often studied separately due to the complexity of the individual problems. Notably, existing approaches often do not guarantee explicitly (i.e., by design) the ability to isolate failures and reconfigure the system operation while satisfying constraints. Furthermore, the time required to isolate failures and reconfigure the system operation may not be a priori bounded or even finite. For example, in [11], a fault-tolerant model predictive control (FTMPC) strategy is developed based on similar to ours set-theoretic considerations, but our approach is based on the reference governor for safe command tracking, and we guarantee explicitly that failures are isolatable and the system can be reconfigured into the new mode within a finite and a priori known duration. We note that in the isolation and reconfiguration phases, the original constraints may need to be temporarily relaxed but the amount of this relaxation is determined by the designer as a part of the offline design process to ensure existence of the solution. For the same reason, in certain modes constraints may need to be tightened to ensure the system state is within the capability of the FDI and reconfiguration scheme and ultimately the next mode controller to handle.

To highlight the contributions, we proposed a set membership-based reference governor-centric FTC strategy that simultaneously (1) guarantees the safe operation in phases of FDI and system reconfiguration and in all normal and failure modes, (2) guarantees abilities and has finite duration that is known before the online operation for isolation and reconfiguration, (3) enables reference tracking, and (4) handles sequential stuck/jammed actuators failures for systems with set-bounded unmeasured disturbances.

The remainder of the paper is structured as follows. First, the system, its operating modes, and constraints are described in Sect. II. Then, Sect. III introduces our approach to FDI and failure mode reconfiguration and the online computations involved, followed by the description of the offline

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

design that guarantees the isolability and reconfigurability in Sect. IV. A numerical example is reported in Sect. V. Concluding remarks are made in Sect. VI.

II. Preliminaries: Operating Modes, System Dynamics and Constraints

A. Operating Modes

Consider a system with N redundant actuators. Each actuator may fail by being stuck/jammed at a constant position. We assume that only one failure can occur at a time, and there is sufficient time between sequential failures for FDI and failure mode reconfiguration. Then, there are $\Omega = 2^N$ possible modes in total, corresponding to different combinations of stuck actuators. Each operating mode is labeled using $M \in \{0, 1, \cdots, \Omega\}$ where, in particular, the normal mode $M = 0$ has all actuators working properly, and the failure mode $M = \Omega$ has all actuators failed.

B. System Dynamics

We consider a system with a set-bounded input disturbance and discuss the open-loop dynamics, stabilizing nominal controllers, and system response representations in what follows.

1) Open-Loop Systems: Discrete-time linear models are considered to represent system dynamics in each mode. Three representations of the dynamics are used as follows:

$$\begin{aligned} x_{k+1} &= A_M x_k + B_M u_k + F_M w_k, && (1)\\ &= A_M x_k + B_{M,\mu}\mu_{M,k} + B_{M,d} d_M + F_M w_k, && (2)\\ &= A_M x_k + B^{\mu}_M u_k + B_{M,d} d_M + F_M w_k, && (3)\\ y_k &= C_M x_k, && (4) \end{aligned}$$

where x_k is the state, y_k is the output, and $w_k \in \mathcal{W}$ is a set-bounded unmeasured input that can represent the disturbance where $\mathcal{W}$ is assumed to be a closed polytope with $0 \in \mathtt{int}\mathcal{W}$. It is assumed that the exact value of the state can be measured without noise. The first representation (1) is a general state-space representation where $u_k \in \mathcal{U}$ is the control input and B_M is the input matrix. In (2), $B_M u_k$ is split into two parts. The first part $B_{M,\mu}\mu_{M,k}$ is for the working actuators where $\mu_{M,k}$ is the vector of the working actuator inputs. The second part $B_{M,d} d_M$ is for the failed actuators where $d_M \in \mathcal{D}_M$ is the vector of constant inputs of the stuck/jammed actuators. For $B^{\mu}_M u_k$ in (3), the columns of B_M corresponding to the failed actuators are set to zero to form B^{μ}_M so that $B^{\mu}_M u_k$ equals $B_{M,\mu}\mu_{M,k}$.

2) Closed-Loop Systems: To stabilize the system and track the given references (where the number of references is assumed to be less than or equal to the number of working actuators), feedback and feedforward control are used to command the working inputs using

$$\begin{aligned} \mu_{0,k} &= K_0 x_k + G_0 v_k,\\ \mu_{M,k} &= K_M x_k + G_M v_k + H_M d_M \ \forall M \in \{1, \cdots, \Omega - 1\}, \end{aligned}$$

where K_M is the stabilizing feedback gain, while G_M and H_M are the feedforward gains for the references and the failed actuator positions that are assumed to be measured or accurately estimated. The system is assumed to be stable in mode Ω when the system runs in open-loop so that safety constraints can be handled by restricting the operation of its predecessor modes.

Then, the closed-loop system can be represented by

$$x_{k+1} = \bar{A}_M x_k + \bar{B}_M U_{M,k} + F_M w_k, \qquad (5)$$

where

$$\begin{aligned} U_{0,k} &= v_k, \quad U_{\Omega,k} = d_\Omega,\\ U_{M,k} &= \begin{bmatrix} v_k \\ d_M \end{bmatrix} \ \forall M \in \{1, \cdots, \Omega - 1\}, \end{aligned}$$

and $\bar{A}_M$ and $\bar{B}_M$ are appropriately defined (see the models in [2] for details).

3) System Response Representations: Let $x_{M,k}$ denote the predicted state of the system at time instant k in mode M. Define, for $k \geq 1$, the set, $\mathcal{Q}_{M,k}$, as a polyhedral overbound on the set of states reachable at time k by applying all possible disturbance sequences when $x_{M,0} = 0$, that is,

$$\begin{aligned} \mathcal{Q}_{M,k} \supseteq\ & B_{M,d}\mathcal{D}_M \bigoplus F_M\mathcal{W} \bigoplus A_M(B_{M,d}\mathcal{D}_M \\ & \bigoplus F_M\mathcal{W}) \bigoplus \cdots \bigoplus A_M^{k-1}(B_{M,d}\mathcal{D}_M \bigoplus F_M\mathcal{W}), \end{aligned} \qquad (6)$$

where $\bigoplus$ stands for the Minkowski sum. Now, consider the nominal prediction of the state with $w_k = 0\ \forall k \geq 0$, $d_M = 0$, and the input command $u^*_k \in \mathcal{U}$. We have

$$x^{\mathtt{u}}_{M,k} = x^{\mathtt{u}}_{M,k}(U^*) = S_{M,k} x_0 + T_{M,k} U^*, \qquad (7)$$

where

$$\begin{aligned} & S_{M,k} = A^k_M,\ T_{M,k} = \begin{bmatrix} A_M^{k-1}B^{\mu}_M & A_M^{k-2}B^{\mu}_M & \cdots & B^{\mu}_M \end{bmatrix},\\ & U^* = \begin{bmatrix} u_0^{*T} & u_1^{*T} & \cdots & u_{k-1}^{*T} \end{bmatrix}^T. \end{aligned}$$

Note that the elements of the input command U^* sequence corresponding to the failed input channels have no impact to the system response since the corresponding columns of B^{μ}_M are zero.

Then, by the superposition principle for linear systems, we have

$$\begin{aligned} x_{M,k} \in \mathfrak{R}_{M,k}(U^*) &= \left\{x^{\mathtt{u}}_{M,k}(U^*)\right\} \bigoplus \mathcal{Q}_{M,k}\\ &= \left\{S_{M,k}x_0 + T_{M,k}U^*\right\} \bigoplus \mathcal{Q}_{M,k}. \end{aligned} \qquad (8)$$

Since $\mathcal{W}$ is a closed polytope, it is reasonable to assume that $\mathcal{Q}_{M,k}$ in (6) are also polytopes. Note that the reachable sets $\mathfrak{R}_{M,k}(U^*)$ are polyhedral if $\mathcal{Q}_{M,k}$ are polyhedral.

C. Constraints

Pointwise-in-time state and control constraints are imposed to ensure safe operation of the system. Since the working actuator input $\mu_{M,k}$ is a function of the state x_k and the closed-loop input $U_{M,k}$, these state and control constraints are transformed into the form:

$$\mathcal{A}^*_M \begin{bmatrix} x_k \\ U_{M,k} \end{bmatrix} \leq \mathcal{b}^*_M,$$

and the safety constraints are further defined by

$$x_k \in \mathcal{X}^*_M(U_{M,k}) = \left\{x :\ \mathcal{A}^*_M \begin{bmatrix} x \\ U_{M,k} \end{bmatrix} \leq \mathcal{b}^*_M\right\}. \qquad (9)$$

To accommodate the sequential failures, the safety constraints of the predecessor modes could be artificially tightened to help the system satisfy the constraints of the subsequent operating modes and during the failure isolation and reconfiguration. On the other hand, the safety constraints could be temporarily relaxed during the failure mode isolation and reconfiguration to, for example, reduce the number of time steps needed during the mode transition, which can help reduce the online computations. The tightened safety constraints during the operation in each mode, as well as the relaxed safety constraints for isolation and reconfiguration are defined as follow:

$$\begin{aligned} x_k \in &\mathcal{X}_M(U_{M,k}) = \mathcal{X}_M^*(U_{M,k}) \cap \bar{\mathcal{X}}_M(U_{M,k}), \\ x_k \in &\mathcal{X}_{I,M}(U_{M,k}), \qquad x_k \in \mathcal{X}_{R,M}(U_{M,k}), \end{aligned}$$

where the sets $\bar{\mathcal{X}}_M(U_{M,k})$, $\mathcal{X}_{I,M}(U_{M,k}) \supseteq \mathcal{X}_M^*(U_{M,k})$, and $\mathcal{X}_{R,M}(U_{M,k}) \supseteq \mathcal{X}_M^*(U_{M,k})$ are to be designed appropriately. One of the easiest way, if all elements of $\mathcal{b}_M^*$ are positive, is to use scaling factors and let

$$x_k \in \mathcal{X}(U_{M,k}) = \Big\{ x : \ \mathcal{A}_M^* \begin{bmatrix} x_k \\ U_{M,k} \end{bmatrix} \leq \eta \mathcal{b}_M^* \Big\}, \tag{10}$$

for $\mathcal{X} = \mathcal{X}_M, \mathcal{X}_{I,M}, \mathcal{X}_{R,M}$ respectively corresponding to $\eta = \eta_{O,M}, \eta_{I,M}, \eta_{R,M}$, where $\eta_{O,M} \in (0, 1]$ and $\eta_{I,M}, \eta_{R,M} \in [1, \infty)$ while they should all be as close to 1 as possible to avoid overly restricted/relaxed operation.

III. Online FDI and Reconfiguration Process

A. Structure Overview

Figure 1 illustrates the online process flow of the FDI and failure mode reconfiguration strategy for the proposed FMEM system with three phases. In phase 0, the failure detection is run at every time step to check if there is a new failure. If the failure is detected, the system enters phase 1 for the failure isolation, at the end of which the failure mode M is known. Otherwise, the system continues operating in phase 0, and a reference governor is used to generate the modified reference v_k for reference tracking without constraint violations. Conversely, during the isolation phase, using a reference sequence is less straightforward than using an open-loop input sequence since the closed-loop dynamics are uncertain without knowing the failure mode M. Instead, a sequence of actuator input commands U^* is computed and applied to the plant. Once the isolation process is over, we know the value of M, and it is assumed that the failure has been identified (i.e. the value of d_M is known). The system moves on to phase 2 where the nominal controller for the isolated mode M is enabled and the reconfiguration process is carried out. A recovery sequence of modified references $\boldsymbol{v}$ is generated, and the system operates with this reference sequence until the end of the reconfiguration process. Then, the system returns to phase 0 and operates in the new mode.

Fig. 1. Structural overview of the online FDI and failure mode reconfiguration strategy.

B. Phase 0: Reference Tracking and Failure Detection

1) Constraint Admissible Sets: We first introduce the definition of a constraint admissible set since both the application of reference governor and the failure detection use this concept. The constraint admissible set of mode $M \in \{0, \cdots, \Omega\}$, denoted by $\mathcal{O}_{\infty,M}$, is defined as a set of the initial state x_0 and the constant closed-loop input U_M such that, with these pairs, the safety constraints given by (10) for $\mathcal{X} = \mathcal{X}_M$ will be satisfied for all future time. We let

$$\begin{aligned} \mathcal{O}_{\infty,M} = \big\{ (U_M, x_0) : \ & x_t \in \mathcal{X}_M(U_M) \ \forall t \in \mathbb{Z}_{\geq 0}, \\ & x_{M,\mathrm{ss}}(U_M) \bigoplus \mathcal{B}_\epsilon \subset \mathcal{X}_M(U_M) \big\}, \end{aligned} \tag{11}$$

where x_t is the system response, $x_{M,\mathrm{ss}}(U_M)$ is the steady-state point (assuming zero-disturbance) given by

$$x_{M,\mathrm{ss}}(U_M) = (I - \bar{A}_M)^{-1} \bar{B}_M U_M,$$

and $\mathcal{B}_\epsilon$ is an open ball of radius $\epsilon > 0$. By this definition, the constraint admissible sets are positively invariant, finitely determined, and can be represented by a finite set of affine inequalities under mild additional assumptions [12].

2) Reference Governor: For mode $M \in \{0, \cdots, \Omega - 1\}$, at every time step k in phase 0, in order to track the reference command r_k as close as possible without violating the safety constraints, a reference governor is used to generate the modified reference v_k by solving the following quadratic programming (QP) problem:

$$\begin{aligned} \min_{v_k} \ & \|r_k - v_k\|_2^2 \\ \text{s.t.} \ & (U_{M,k}, x_k) \in \mathcal{O}_{\infty,M}. \end{aligned} \tag{12}$$

The modified reference v_k is then taken by the controller to command the input of the working actuators.

3) Failure Detection: If the system is operating in the current mode M_0 and the control input is u_k, the state x_{k+1} is determined by (1) with $M = M_0$. Hence, if the condition

$$x_{k+1} \notin A_{M_0} x_k + B_{M_0} u_k \bigoplus F_{M_0} \mathcal{W} \tag{13}$$

holds, a new actuator failure has occurred and the isolation phase is initiated. In the isolation phase, the successor modes of mode M_0, whose set is denoted by $\mathrm{succ}(M_0)$, are considered. Note that it is possible that (13) does not hold but the new failure has already happened as the disturbance $w_k \in \mathcal{W}$ can mask the failure. However, since the system

response is close to nominally expected, the operation is considered to be safe in this case.

C. Phase 1: Failure Isolation

1) Isolability: Once a new failure is detected, the system enters the failure isolation phase, at the end of which the failure mode M should be known. Consider mode $M_0 \in \{0, \cdots, \Omega-1\}$ whose successor mode is not $M = \Omega$ (otherwise it is certain that $\text{succ}(M_0) = \{\Omega\}$), and any two candidate modes $M_1, M_2 \in \text{succ}(M_0)$ where $M_1 \neq M_2$. Based on the measured state, it is sufficient to isolate the failure in N_I steps if there exists an isolation sequence U^* such that the reachable sets have no common states, i.e.,

$$\mathfrak{R}_{M_1,N_I}(U^*) \bigcap \mathfrak{R}_{M_2,N_I}(U^*) = \emptyset. \tag{14}$$

Then, the failure mode is the one whose reachable set contains the measured state x_{N_I}.

Following (8), condition (14) can be ensured if and only if

$$\begin{aligned}&(S_{M_1,N_I} - S_{M_2,N_I})x_0 + (T_{M_1,N_I} - T_{M_2,N_I})U^* \\ &\quad \notin \mathcal{Q}_{M_2,N_I} \bigoplus (-\mathcal{Q}_{M_1,N_I}),\end{aligned} \tag{15}$$

where x_0 here represents the state at the beginning of the isolation.

2) Computations to Generate the Isolation Sequence: By the definition of $\mathcal{Q}_{M,k}$, the set on the right-hand-side of (15) is polyhedral. Consider its representation in the form of affine inequalities:

$$\mathcal{Q}_{M_2,N_I} \bigoplus (-\mathcal{Q}_{M_1,N_I}) = \{x : \ \mathcal{H}_j x \leq \hbar_j, \ j = 1, \cdots, q\}.$$

Then, (15) can be re-stated as

$$\begin{aligned}\exists j : \mathcal{H}_j \big(&(S_{M_1,N_I} - S_{M_2,N_I})x_0 \\ &+ (T_{M_1,N_I} - T_{M_2,N_I})U^* \big) > \hbar_j.\end{aligned} \tag{16}$$

The problem becomes finding an isolation sequence U^* such that (16) holds, and at the same time, the safety constraints given by (10) for $\mathcal{X} = \mathcal{X}_{I,M}$ are satisfied. This can be handled using mixed-integer optimization applied to (16) transformed using the "Big-M" technique (see Sect. 9.3.1 in [13]). We introduce binary integers $\delta_j \in \{0,1\}, j = 1, \cdots, q$. The condition (16) can be written as

$$\begin{aligned}&\sum_{j=1}^{q} \delta_j \geq 1, \\ &\mathcal{H}_j \big((S_{M_1,N_I} - S_{M_2,N_I})x_0 + (T_{M_1,N_I} - T_{M_2,N_I})U^* \big) \\ &\quad \geq \hbar_j - (1-\delta_j)\mathbb{M} + \gamma \quad \forall j \in \{1, \cdots, q\},\end{aligned} \tag{17}$$

where $\mathbb{M} \gg 0$ is a large positive number, and $\gamma > 0$ is a small positive number introduced to replace "$>$" with "$\geq$". For the numerical example in Sect. V, we use $\mathbb{M} = 10^9$ and $\gamma = 10^{-6}$.

The constraints (17) can now be integrated into a mixed-integer quadratic programming (MIQP) problem, whose objective is to determine a minimum norm control sequence U^* that ensures the ability to distinguish the operation in mode M_1 versus operation in mode M_2 without violating the safety constraints, that is, to find the solution of the following problem:

$$\begin{aligned}&\min_{U^*, \delta_1, \cdots, \delta_q} \ \|U^*\|_2^2 \\ &\text{s.t.} \ \ (U^*, \delta_1, \cdots, \delta_q, x_0) \in \mathcal{C}(M_0),\end{aligned} \tag{18}$$

where

$$\begin{aligned}&\mathcal{C}(M_0) = \mathcal{C}_{M_1,M_2} = \Big\{ (U^*, \delta_1, \cdots, \delta_q, x_0) : \\ &\forall j \in \{1, \cdots, q\}, \ \delta_j \in \{0,1\}, \ \sum_{j=1}^{q} \delta_j \geq 1, \\ &\mathcal{H}_j (T_{M_1,N_I} - T_{M_2,N_I})U^* - \mathbb{M}\delta_j \\ &\quad + \mathcal{H}_j (S_{M_1,N_I} - S_{M_2,N_I})x_0 \geq \hbar_j - \mathbb{M} + \gamma, \\ &\forall t \in \{1, \cdots, N_I\}, x_t \in \mathcal{X}_{I,M_1}(U_{M,t}), x_t \in \mathcal{X}_{I,M_2}(U_{M,t}) \Big\}.\end{aligned} \tag{19}$$

Remark 1. If there are more than two candidate modes, constraints can be defined similar to (19) for all distinct pairs of candidate modes, e.g., if the candidate modes are $M = 1, 2, 3$, then constraints should be defined for mode pairs $(1,2)$, $(2,3)$ and $(3,1)$. The MIQP problem becomes

$$\begin{aligned}&\min \ \|U^*\|_2^2 \\ &\text{s.t.} \ \ (U^*, \delta_{1,2,1}, \cdots, \delta_{1,2,q_1}, \delta_{2,3,1}, \cdots, \delta_{2,3,q_2}, \\ &\qquad \delta_{3,1,1}, \cdots, \delta_{3,1,q_3}, x_0) \in \mathcal{C}(M_0),\end{aligned}$$

where $\mathcal{C}(M_0) = \mathcal{C}_{1,2} \cap \mathcal{C}_{2,3} \cap \mathcal{C}_{3,1}$.

D. Phase 2: Failure Reconfiguration

When the system finished operating with the isolation sequence, it enters the reconfiguration phase with the known failure mode $M \in \{1, \cdots, \Omega-1\}$ and the vector of stuck/jammed actuator positions d_M that has been identified. In this phase, a reference sequence $\boldsymbol{v} = \begin{bmatrix} v_0^T & \cdots & v_{N_M}^T \end{bmatrix}^T$ is generated to steer the state into the state projection of the constraint admissible set, $\text{Proj}_x \mathcal{O}_{\infty,M}$, within N_M steps without violating the relaxed safety constraints given by (10) for $\mathcal{X} = \mathcal{X}_{R,M}$. The recovery reference sequence is determined by solving the following QP problem:

$$\begin{aligned}&\min_{\boldsymbol{v}} \ \|r_0 \mathbf{1} - \boldsymbol{v}\|_2^2 \\ &\text{s.t.} \quad x_t \in \mathcal{X}_{R,M}(U_{M,t}) \ \ \forall t \in \{0, \cdots, N_M - 1\}, \\ &\qquad (U_{M,N_M}, x_{N_M}) \in \mathcal{O}_{\infty,M},\end{aligned} \tag{20}$$

where $t = 0$ here corresponds to the beginning of the reconfiguration phase, and by using $r_0 \mathbf{1}$ it is assumed that the reference command stays at constant during the reconfiguration process. The system eventually returns to phase 0 once it finished operating with the recovery sequence.

IV. Conditions for Guaranteed Failure Isolation and Reconfiguration

The set-membership conditions for the offline design procedure is now described. So far, three optimization problems, (12), (18), and (20), have been introduced for different online phases of the FMEM strategy. For the reference governor defined by (12), the problem is feasible in the failure modes because of the constraint $(U_{M,N_M}, x_{N_M}) \in \mathcal{O}_{\infty,M}$ imposed

in (20). To ensure the feasibility of failure mode isolation and reconfiguration, i.e., for (18) and (20), we can choose the number of steps allowed for isolation N_I, the number of steps allowed for reconfiguration N_M, and the safety constraint scaling coefficients $\eta_{O,M}$, $\eta_{I,M}$, and $\eta_{R,M}$.

A. Isolation Conditions

When the system is operating in mode $M_0 \in \{0, \cdots, \Omega - 1\}$, its state is contained in $\text{Proj}_x \mathcal{O}_{\infty,M_0}$, but when a failure is detected, the state is in the following set:

$$\mathcal{I}_{M_0} = \bigcup_{M \in \text{succ}(M_0)} A_M \text{Proj}_x \mathcal{O}_{\infty,M_0} \bigoplus B_M \mathcal{U} \bigoplus F_M \mathcal{W}. \tag{21}$$

This implies the following result:

Proposition 1 (Isolation Condition)**.** *If the following condition holds,*

$$\mathcal{I}_{M_0} \subseteq \mathit{Proj}_x \mathcal{C}(M_0), \tag{22}$$

then (18) *is feasible.*

B. Reconfiguration Conditions

We begin by introducing the recoverable sets, which, for the successor modes $M \in \text{succ}(M_0)$, are defined as

$$\begin{aligned} \mathcal{R}^{N_M}_{\infty,M}(d_M) = \big\{ & x_0 : \exists \{v_0, \cdots, v_{N_M}\} \text{ such that} \\ & x_t \in \mathcal{X}_{R,M}(U_{M,t}) \ \forall t \in \{0, \cdots, N_M - 1\}, \\ & (U_{M,N_M}, x_{N_M}) \in \mathcal{O}_{\infty,M} \big\}. \end{aligned} \tag{23}$$

In mode Ω, we let the recoverable set to be the state projection of the constraint admissible set, that is,

$$\mathcal{R}^{N_\Omega}_{\infty,\Omega} = \text{Proj}_x \mathcal{O}_{\infty,\Omega} \quad \forall N_\Omega \geq 0, \tag{24}$$

as the system runs open-loop when all actuators have failed.

At the end of the isolation phase, i.e., the beginning of the reconfiguration phase, the system is in the known failure mode M, and the states are in

$$\mathcal{S}'_M(d_M, U^*) = \{x_{N_I} : \ x_0 \in \text{Proj}_x \mathcal{C}(M_0)\}, \tag{25}$$

where x_{N_I} results from using the isolation sequence U^* assuming the stuck/jammed actuator input is d_M. Furthermore, since the state at the beginning of the isolation $x_0 \in \mathcal{I}_{M_0}$, if the isolation condition (22) holds, the states are contained in

$$\mathcal{S}''_M(d_M, U^*) = \{x_{N_I} : \ x_0 \in \mathcal{I}_{M_0}\}. \tag{26}$$

If we have

$$\mathcal{S}''_M(d_M, U^*) \subseteq \bigcap_{d_M \in \mathcal{D}_M} \mathcal{R}^{N_M}_{\infty,M}(d_M), \tag{27}$$

which implies that the state at the end of the isolation phase is in the recoverable set for any stuck/jammed actuator position, the optimization problem (20) is guaranteed to be feasible. However, d_M and U^* are a priori unknown. To satisfy (27), it is sufficient to define

$$\mathcal{S}(M_0) = \{x_{N_I} : \ x_0 \in \mathcal{I}_{M_0}, \ U^* \in \mathcal{U}^{N_I}, \ d_M \in \mathcal{D}_M\}, \tag{28}$$

i.e., the set of states that are N_I steps later of the states in $\mathcal{I}_{M_0}$ considering all possible inputs (for both working and failed actuators) and disturbances, and impose a stricter condition as

$$\mathcal{S}(M_0) \subseteq \bigcap_{d_M \in \mathcal{D}_M} \mathcal{R}^{N_M}_{\infty,M}(d_M). \tag{29}$$

Proposition 2 (Reconfiguration Condition)**.** *If the conditions* (22) *and* (29) *hold, then* (20) *is feasible.*

The offline design procedure to satisfy the conditions of Propositions 1 and 2 is demonstrated through a numerical example in the next section.

V. Numerical Example

A. System Dynamics and Operating Modes

A mass-spring-damper system extended to consider set-bounded input disturbance based on the numerical example in [7] is used for illustration. The system is represented by

$$\dot{x} = Ax + Bu + Fw, \quad y = Cx, \tag{30}$$

where $x = [\alpha \ \ \lambda]^T$ is the state vector of the displacement α and the velocity λ, $u = [f_1 \ \ f_2]^T$ is the input vector of two forces, and $F = [0 \ \ \frac{1}{m_0}]^T$ where m_0 is the mass. The details about the open-loop model, the process to acquire the controllers using the Linear Quadratic Regulator (LQR) theory, and the definitions of operating modes follow [7] so they are not repeated here.

B. Constraints

The state and control constraints are given by

$$|\alpha| \leq \alpha_{\max}, \ |f_1| \leq f_{1_{\max}}, \text{ and } |f_2| \leq f_{2_{\max}}, \tag{31}$$

where $\alpha_{\max} = 1$, $f_{1_{\max}} = 0.6$, and $f_{2_{\max}} = 0.4$. In addition, the input disturbance is bounded by

$$|w| \leq w_{\max}, \tag{32}$$

where $w_{\max} = 0.02$.

C. Offline Design for Guaranteed Isolability and Reconfigurability

In this section, we consider the case of sequential failures where the system begins operating in mode 0, then changes to mode 1 where f_2 fails, and eventually finishes in mode 3 with both actuators failed. The case with 0-2-3 mode transition sequence follows a similar procedure (in mode 2, f_1 fails while f_2 is normal). The `Bensolve` toolbox [14] is used for polyhedral computations. The design parameters, N_I, N_M, $\eta_{O,M}$, $\eta_{I,M}$ and $\eta_{R,M}$, are chosen from a grid of values to minimize the number of time steps needed and the changes from the original constraints due to scaling.

The offline design proceeds backward in terms of the failure sequence, that is, we begin by considering mode 3 and determining its recoverable set given the safety constraints. To ensure the system state is in $\text{Proj}_x \mathcal{O}_{\infty,3}$ during mode 1, we choose $\eta_{O,1} = 0.45$ to satisfy $\text{Proj}_x \mathcal{O}_{\infty,1} \subseteq \text{Proj}_x \mathcal{O}_{\infty,3}$. The result is shown in Fig. 2(c). For mode 2, $\eta_{O,2} = 0.75$.

Next, the isolability condition for the transition from mode 0 given by (22) with $M_0 = 0$ is considered. We let $\eta_{O,0} = 1$ so that the normal operation is not artificially restricted, and we use $\eta_{I,1} = 1.2$ to relax the safety constraints for $N_I = 2$ steps during the isolation phase. Note that this is a common step for the 0-1-3 and 0-2-3 mode transitions, as both mode 1 and 2 are the successor modes of mode 0. Hence, the parameters N_I, $\eta_{I,1}$ and $\eta_{I,2}$ are adjusted together to satisfy (22). For mode 2, we also let $\eta_{I,2} = 1.2$. Figure 2(a) illustrates the set-membership relation.

Finally, we consider the reconfigurablity for the mode transition to $M = 1$. The recoverable set of mode 1 is determined following (23), and the condition that needs to be satisfied is (29). In this phase, we relax the safety constraints by having $\eta_{R,1} = 1.7$ and allow $N_1 = 15$ steps for the recovery. The set-membership relation is shown in Fig. 2(b). For mode 2, $\eta_{R,2} = 1.9$ and $N_2 = 22$.

D. Simulations

A simulation is run for the case of 0-1-3 mode transition. The input disturbance follows a normal distribution within $\mathcal{W}$ using zero mean and the standard deviation $\sigma = w_{\max}/6$. The failures are set to happen in 2 and 44 sec, while the displacement reference command switches between -0.99 and 0.99 in 20 and 40 sec. Figure 2(c) shows the state trajectory and Fig. 2(d) shows the time-based signals for a 60-sec simulation. Both failures are detected in one step and the isolation and reconfiguration takes 3.4 sec in total as determined by N_I and N_M for $M = 1$. The difference between the reference command and the modified reference in mode 1 shows that the operation is restricted after the initial failure to prepare for the potential subsequent failure, i.e., transiting to mode 3, which makes the system run in open-loop. No constraint violations are observed during the operation in any of the modes and phases.

Fig. 2. (a) Isolation condition satisfied for $M_0 = 0$. (b) Reconfiguration conditions satisfied for $M_0 = 0$. (c) State projections of $\mathcal{O}_{\infty,M}$ and state trajectory. (d) Time-based signals where M is the actual mode and M_{est} stands for the mode determined by the FMEM unit.

VI. Concluding Remarks

Enhancements to a reference governor-based Failure Mode and Effect Management (FMEM) strategy for a system with redundant actuators that can become stuck/jammed have been developed. These enhancements ensure the ability to detect and isolate failures within a finite time while tracking reference commands and satisfying state and control constraints. Conditions have been derived that can be used in the offline design phase to guarantee the ability to detect and isolate failures within a pre-determined time duration and to reconfigure the system into the next mode. The proposed system can handle sequential failures and unmeasured set-bounded disturbance inputs. A mass-spring damper example with two force inputs has been reported to illustrate the design and operation of the proposed FMEM strategy. Possible directions of future work include considering (1) other types of failures, e.g., failures caused by actuator efficiency degradation, failed signals that change slowly with bounded rates, and failures related to sensors and/or communication, and (2) challenges for implementing the strategy in real-time, e.g., in the situation when the isolation and reconfiguration sequences cannot be generated in time for execution due to limitations of computational resources.

References

[1] H. Williamson, *Air crash investigations: Jammed rudder kills 132, the crash of USAir Flight 427*. lulu.com, October 2011.

[2] H. Li, I. Kolmanovsky, and A. Girard, "Set-theoretic failure mode reconfiguration for stuck actuators," *IEEE Control Systems Letters*, vol. 6, pp. 1316–1321, 2021.

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

[4] I. Hwang, S. Kim, Y. Kim, and C. E. Seah, "A survey of fault detection, isolation, and reconfiguration methods," *IEEE transactions on control systems technology*, vol. 18, no. 3, pp. 636–653, 2009.

[5] M. Hosseinzadeh, I. Kolmanovsky, S. Baruah, and B. Sinopoli, "Reference governor-based fault-tolerant constrained control," *arXiv preprint arXiv:2107.08457*, 2021.

[6] 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.

[7] H. Li, I. Kolmanovsky, and A. Girard, "A failure mode reconfiguration strategy based on constraint admissible and recoverable sets," in *2021 American Control Conference (ACC)*, pp. 4771–4776, IEEE, 2021.

[8] 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.

[9] 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.

[10] A. Abbaspour, S. Mokhtari, A. Sargolzaei, and K. K. Yen, "A survey on active fault-tolerant control systems," *Electronics*, vol. 9, no. 9, p. 1513, 2020.

[11] D. M. Raimondo, G. R. Marseglia, R. D. Braatz, and J. K. Scott, "Fault-tolerant model predictive control with active fault isolation," in *2013 Conference on Control and Fault-Tolerant Systems (SysTol)*, pp. 444–449, IEEE, 2013.

[12] 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.

[13] H. P. Williams, *Model building in mathematical programming*. John Wiley & Sons, 2013.

[14] 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.