A Convex Approach to Fault Tolerant Control

Peiman G. Maghami
NASA Goddard Space Flight Center, Greenbelt, MD 20771

David E. Cox
NASA Langley Research Center, Hampton, VA 23681

The design of control laws for dynamic systems with the potential for actuator failures is considered in this work. The use of Linear Matrix Inequalities allows more freedom in controller design criteria than typically available with robust control. This work proposes an extension of fault-scheduled control design techniques that can find a fixed controller with provable performance over a set of plants. Through convexity of the objective function, performance bounds on this set of plants implies performance bounds on a range of systems defined by a convex hull. This is used to incorporate performance bounds over a variety of soft and hard failures into the control design problem.

Introduction

The control design of lightly damped dynamic systems is a challenging area for incorporating fault tolerance. Loss of an actuator or sensor can greatly degrade, or even destabilize, the closed-loop performance. This is particularly true for optimal control laws that are tuned to a specific operating condition. Although robust control can account for real parametric uncertainty, in the case of full actuator failure the use of broadband 100% input uncertainty severely limits loop gains, and often results in conservative control laws.

An alternative approach is considered here that makes use of the flexibility offered by posing control design problems as Linear Matrix Inequalities (LMIs). The use of LMIs in control theory has been studied extensively in recent years. Of particular interest is the design of linear parameter varying (LPV) control laws, that are implicitly gain scheduled with changes in the plant. One application of LPV control is in the design of fault-scheduled (FS) controllers which are scheduled with measured fault parameters in the system. Here we examine a modification to the FS control design that allows for fixed controllers and removes the need for griding the parameter space.

The design technique is tested on a simple coupled mass-spring-damper system. Although quite simple this system possesses the same qualitative characteristics as more complex flexible body systems. Controllers are designed using the proposed LMI framework and analyzed under various fault conditions. These faults include hard failure - a complete loss of an actuator and soft failures - dynamically altered capability of an actuator.

Control Synthesis

Much progress has been made in the synthesis of control laws as convex optimization problems, and software to solve such problems is becoming more widely available. One benefit of this approach is that equations for the analysis of linear systems, can be written quite naturally as linear matrix inequalities. With the proper change of variables these analysis equations can be transformed directly into synthesis equations for controllers that meet the closed-loop objectives. This allows multi-objective problems involving a collection $H_2$ or $H_{\infty}$ norms, as well as regional pole placement, passivity, and other performance objectives.

A second, and here more significant, benefit of using LMIs to pose controller synthesis equations is that performance criteria can be simultaneously imposed on multiple plant models. This allows potential failure conditions to be explicitly defined in the design process, and predictions made about performance under nominal, as well as degraded conditions. For soft failures and dynamic degradation, it is important to guarantee performance not only at specific conditions, but over a range of possible variations. The convexity of the LMI controller synthesis equations allows this problem of infinite constraints to be bounded by a finite set of conditions imposed at vertex systems.

The basis of the control synthesis in this work is an $H_2$ design problem. That is, find $K$ that minimizes $\|F_l(P,K)\|_2$, where $F_l$ is the lower Linear Fractional Transformation. The augmented plant model $P$ is partitioned with disturbance to performance path, $F_{uv}$, over the actuator to sensor path, $F_{vu}$, as $P = \begin{bmatrix} P_{uv} & P_{vu} \end{bmatrix}$. A block diagram of the closed-loop system, indicating the feedback structure of the plant, controller, and design weightings is shown in Figure 1. The performance requirement is defined in terms of the
weighted transfer function from disturbances to the performance output. Additional paths are included in the augmented system model to account for the cost of control effort, weighted by $W_u$, and the presence of disturbance input at the sensors, weighted by $W_v$. With constant weightings this arrangement gives the $H_2$ problem essentially the same design parameters as a traditional Linear Quadratic Gaussian (LQG) control law.\(^\text{10}\)

Solving the $H_2$ control problem via Riccati equations is a straightforward procedure, however, it lacks the ability to account for failure conditions in the design. Calculation of the $H_2$ norm using LMIs involves finding a $P > 0$ and $Q = Q^T$ that minimizes $\text{Tr}(Q)$, and satisfies,

$$
\begin{bmatrix}
AP + PA & PB_w \\
B_w^TP & -I
\end{bmatrix} < 0,
\begin{bmatrix}
P & C_T \\
C & Q
\end{bmatrix} > 0
$$

where $(A,B,C)$ is a realization of the closed-loop system $F_r(q, K)$. As an analysis LMI this is readily solved for $P$ and $Q$, however, $(A,B,C)$ is the closed-loop system and it contains further unknowns from the control law. A direct expansion of (1) yields inequalities that contain products of unknowns, and therefore is no longer convex.

As developed in\(^\text{7}\) a congruence transformation coupled with a substitution of variables can restore convexity with respect to a new set of unknowns. These unknowns are $(A, B, C, D, X, Y)$ and are related to the original controller $(A_k, B_k, C_k, D_k)$ and Lyapunov term $P$ by the following equations,

$$
\begin{align*}
\dot{A} &= N A_k M^T + N B_k C X + Y B C_k M^T \quad (2) \\
\dot{B} &= N B_k + Y B D_k \\
\dot{C} &= C_k M^T + D_k C X \\
\dot{D} &= D_k
\end{align*}
$$

where $M N^T = (I - XY)$ and $P$ is related to $X$ and $Y$ by

$$
P \begin{bmatrix} X & I \\ M^T & 0 \end{bmatrix} = \begin{bmatrix} I & Y \\ 0 & N^T \end{bmatrix}.
$$

In these new unknowns the $H_2$ norm condition of (1) can be written as the equivalent problem of minimizing the trace of $Q$ subject to

$$
\begin{bmatrix}
AX + B \dot{C} + (\cdot)^T \\
A + (A + BD_k C)^T Y & A + B \dot{C} + (\cdot)^T \\
(B_w + BD_k D_y)^T Y B_w & (B_w + BD_k D_y)^T - I
\end{bmatrix}< 0
$$

where $\begin{bmatrix} X & Y \\ I & 0 \end{bmatrix} > 0$ (8)

$$
\begin{bmatrix}
C_x X + D_x \dot{C} & C_y + D_y \dot{D} \\
C_x + D_x \dot{C} & Q
\end{bmatrix}
$$

where the terms $(\cdot)^T$ are implied by symmetry of the overall matrix. As Linear Matrix Inequalities, these conditions represent convex constraints on the solution space. This has two advantages. First solutions to convex problems are numerically tractable, even with the large number of unknowns inherent in an output feedback problem. Interior-point algorithms are available that can solve such problems or show that a solution does not exist.

The second advantage is that convex functions, when evaluated over convex hulls, reach their maximum at a vertex point. This means that ensuring these conditions over a infinite range of parameter variation is possible by checking only a a finite set of well chosen vertex models. For example, if a set of unknowns were found for multiple state input matrices, i.e. $B = \{B_1, B_2\}$, then the resulting controller would have performance guarantees not only for the systems realized by $(A, B_1, C, D)$ and $(A, B_2, C, D)$ but also for any input matrix given by,

$$
B(\alpha) = \alpha B_1 + (1-\alpha) B_2, \quad 0 \leq \alpha \leq 1
$$

This condition ensures tolerance of attenuation in actuator gain as well as fully failed scenarios.

Eliminating Parametric Dependence

The design method described above yields fault-scheduled (FS) control laws. This is because even for a constant set of solution variables $(\hat{A}, \hat{B}, \hat{C}, \hat{D}, X, Y)$ the controller still must be calculated by inversion of (3)-(5), yielding

$$
\begin{align*}
A_k &= N^{-1}(\hat{A} - NB_k CX - YBC_k M^T) - Y(A + BD_k C)X M^{-T} \\
B_k &= N^{-1}(\hat{B} - YBD_k) \\
C_k &= (\hat{C} - D_k CX)M^{-T} \\
D_k &= \hat{D}
\end{align*}
$$

This solution introduces a parametric dependence in the control law. If the input faults of the system are available for real time implementation, then the FS controller can be implemented. The ability to accurately measure faults in a system, however, is often unrealistic. Recent work has looked at sensitivity to errors in the scheduling parameter in an attempt to design robust LPV controllers that will tolerate errors in estimation of the fault condition.\(^\text{11}\)

Here we seek a method to find a fixed controller that will tolerate rapid and unmeasured changes in the condition of the plant. To do this requires enforcing the performance criteria not only at the nominal solution condition but also within a specific neighborhood of that solution. Specifically, we consider systems without disturbance to performance feed-through, i.e. $D_{zw} = 0$. This yields finite open-loop $H_2$ norms and strictly proper optimal controllers, i.e. $\hat{D} = D_k = 0$. A second, and somewhat more restrictive assumption, is that all fault conditions enter the plant model only through changes in the $B$ matrix and these changes
can be bounded by the convex hull of a set of vertex matrices,

\[ B = B_0 + \Delta B, \quad \Delta B \in \text{Co}[\Delta B_1, \Delta B_2, \ldots, \Delta B_n] \]  

(15)

where the convex hull is defined as,

\[ \text{Co}[\Delta B_1, \Delta B_2, \ldots, \Delta B_n] = \sum_{i=1}^{n} \alpha_i \Delta B_i, \quad \forall \alpha_i > 0, \sum_{i=1}^{n} \alpha_i = 1; \]  

(16)

Under these conditions the terms \( \hat{B}, \hat{C}, \hat{A}, X, Y \) are independent of changes in \( B \) and thus remain constant with failures. It is only the term \( \hat{A} \) that must change with the plant changes. Normally, the term \( \hat{A} \) is held constant by corresponding changes in the control law achieved through gain scheduling. The alternative pursued below is to pose additional LMI equations that explicitly account for potential changes in \( \hat{A} \). The norm bounds will hold for the variations in \( \hat{A} \) if synthesis LMIs are posed at the extremal values of \( \hat{A} \). For a single failure mode \( B \equiv \{B_0, B_0 + \Delta B_1\} \) the synthesis LMIs would be

\[
\begin{bmatrix}
AX + B_0 \hat{C} + (\cdot)^T \\
\hat{A} + A^T \\
B_w^T
\end{bmatrix}
\begin{bmatrix}
YA + \hat{B}C + (\cdot)^T \\
Y \hat{A} + \hat{B}C + (\cdot)^T \\
YA + \hat{B}C + (\cdot)^T
\end{bmatrix}
\begin{bmatrix}
(\cdot)^T \\
(\cdot)^T \\
I
\end{bmatrix}
< 0
\]

(17)

\[
\begin{bmatrix}
AX + (B_0 + \Delta B_1) \hat{C} + (\cdot)^T \\
\hat{A} + Y \Delta B_1 \hat{C} + A^T \\
B_w^T
\end{bmatrix}
\begin{bmatrix}
YA + \hat{B}C + (\cdot)^T \\
YA = \hat{B}C + (\cdot)^T \\
YA + \hat{B}C + (\cdot)^T
\end{bmatrix}
\begin{bmatrix}
(\cdot)^T \\
(\cdot)^T \\
-I
\end{bmatrix}
< 0
\]

(18)

\[
\begin{bmatrix}
X \\
I \\
C_z \hat{X} + D_{zv} \hat{C} \\
C_z \\
Q
\end{bmatrix}
\begin{bmatrix}
(\cdot)^T \\
(\cdot)^T \\
(\cdot)^T \\
(\cdot)^T \\
(\cdot)^T
\end{bmatrix}
< 0
\]

(19)

where the variation terms involving \( \Delta B_1 \) has been included in (18). These conditions will provide \( H_2 \) performance with a fixed control law under both the nominal and failed system conditions. However, the synthesis problem is no longer convex as the product of two unknowns, \( Y \) and \( \hat{C} \), appear in (18).

To work around the loss of convexity a two stage approach is taken for the design.

- A robust fault-scheduled control law is first formulated in the LMI framework. For the single failure mode example, this means that in the synthesis LMI Eq. (17) is used as is, however Eq. (18) is modified as follows

\[
\begin{bmatrix}
AX + (B_0 + \Delta B_1) \hat{C} + (\cdot)^T \\
\hat{A} + A^T \\
B_w^T
\end{bmatrix}
\begin{bmatrix}
YA + \hat{B}C + (\cdot)^T \\
YA = \hat{B}C + (\cdot)^T \\
YA + \hat{B}C + (\cdot)^T
\end{bmatrix}
\begin{bmatrix}
(\cdot)^T \\
(\cdot)^T \\
-I
\end{bmatrix}
< 0
\]

(20)

- The value of matrix \( \hat{C} \), obtained from the LMI synthesis in the first step, and referred to as \( \hat{C}_{\text{opt}} \), is then fixed and a second robust LMI problem is solved, using the degrees of freedom in the remaining variables. The synthesis LMI is defined by Eqs. (17) and (19), along with a modified Eq. (18).

\[
\begin{bmatrix}
AX + (B_0 + \Delta B_1) \hat{C}_{\text{opt}} + (\cdot)^T \\
\hat{A} + Y \Delta B_1 \hat{C}_{\text{opt}} + A^T \\
B_w^T
\end{bmatrix}
\begin{bmatrix}
YA + \hat{B}C + (\cdot)^T \\
YA = \hat{B}C + (\cdot)^T \\
YA + \hat{B}C + (\cdot)^T
\end{bmatrix}
\begin{bmatrix}
(\cdot)^T \\
(\cdot)^T \\
-I
\end{bmatrix}
< 0
\]

(21)

Although this sacrifices the full sense of optimality in the robust controller it does provide a quantitative measure of the performance degradation incurred in accommodating the failure case. Furthermore, it allows a different set of objectives to be imposed in the second stage. This can be used to enforce as a constraint the minimal performance level under failure, and optimize on the nominal, or if desired constrain the nominal and optimize for failure conditions. The freedom to tailor a problem formulation to meet such design criteria has powerful engineering significance, and is one of the advantageous of feasible LMI design methods versus more conventional robust and optimal control.

Defining Vertex Points

Thus far, the paper has described an LMI-based synthesis procedure for designing fixed fault-accommodating controllers which can handle actuator faults/failures. The formulation covers both hard failures, in the form of the total loss of one actuator, as well as soft failures, which represents a degradation in the actuator performance, e.g., loss of bandwidth. As mentioned earlier, the input uncertainties in the LMI framework need only be considered at the vertex points of the parameter space. This is because convex functions, when evaluated over convex hulls, reach their maximum at a vertex point. The number of vertex points generally depends on the nature of the fault/failure being considered. To elaborate on...
this, consider an example of a system with two inputs. First consider a hard failure case, wherein one actuator has totally failed. There are three distinct vertex points that need to be considered in this case. These are: (a) Both actuators functional; (b) Actuator one has failed; and (c) actuator two has failed. Mathematically, these case are described by the following input matrices:

\[ B_0 = B_0; \quad B_1 = [0 \hspace{1cm} B_2^1]; \quad B_2 = [B_0^0 \hspace{1cm} 0] \]  

(22)

where \( B_0^1 \) and \( B_2^1 \) represent the first and second column of \( B_0 \), respectively. The soft failure case is a bit more involved because both gain and phase changes are possible. As mentioned previously, one of the assumptions of the proposed approach is that all fault conditions enter the plant through the state input matrix \( B \). To accommodate this condition, an arbitrary number of vertex points are chosen for each actuator failure. Moreover, corresponding to each vertex point, an LTI filter (with arbitrary dynamics) is selected and placed in series (at the input) with the plant. These filters represent designer-specified soft failure modes (note that even hard failures may be defined as well), whose combination determines the degree of soft failure allowed in the design process. One possible way of implementing the soft failure filters is to increase (for each actuator) the number of independent soft failure filters for that actuator by duplicating the proper column of the \( B_0 \) matrix. In the two-input example, let's assume that for each actuator two independent soft failure modes are being contemplated. Assume that these failures are represented by filters \( F_{11}(s) \), \( F_{12}(s) \), \( F_{21}(s) \), and \( F_{22}(s) \). Let \( \hat{P}(s) \) denote the plant with inflated inputs. Here, \( \hat{P}(s) \) is identical to the nominal plant except it has two additional inputs, identical to the nominal inputs, i.e., \( B = \{B_0 \hspace{1cm} B_2\} \). Now, an augmented plant \( \hat{P}(s) \) may be defined by placing the filter dynamics in series with \( \hat{P}(s) \).

\[ \hat{P}(s) = \hat{P}(s) \text{diag}[F_{11}(s) \hspace{1cm} F_{12}(s) \hspace{1cm} F_{21}(s) \hspace{1cm} F_{22}(s)] \]  

(23)

Now that the soft failure filter dynamics are included in the plant dynamics, the vertex points for the LMI design may be defined by appropriately choosing a constant distribution matrix \( L_i \) for each vertex \( i \) to incorporate a specific failure scenario. Note that the matrix \( L_i \) must be dimensioned such that it reduces the number of inputs back to the original value.

**Example Problem**

The proposed fault tolerant method is demonstrated on a simple mass-spring-damper system. As shown in Figure 3, three serially connected masses compose the system model, with the following parameters: each mass is 1 Kg, each spring is 100 N/m, and each damper is 0.25 Ns/m. A velocity sensor is assumed to provide velocity measurements from mass no. 1. Two force actuators are assumed, at mass no. 1 and 3, to provide control forces. The model can be explicitly written,

\[ \begin{bmatrix} A & B \\ C & D \end{bmatrix} = \begin{bmatrix} 0 & I \\ M^{-1}K & M^{-1}C \\ I & 0 \\ 0 & 0 \end{bmatrix} \]  

(24)

The failures of interest are soft failures, in terms of gain attenuation or phase changes, in any single actuator, up to hard failures, i.e., a full loss of any single input. The spring-mass system is assumed to be disturbed by an unmeasured force applied to the second mass. The goal of the controller is to minimize the \( H_2 \) norm from this input to a performance metric which is the sum of the the displacement and velocity of the third mass. This represents the ability of the disturbance to drive energy into the system. The optimization is balanced by including both sensor noise, as additional weighted disturbances, and a control effort penalty. This arrangement is shown in the augmented plant of Figure 1.

To accommodate both soft and hard failures in the same parameterization, first the two inputs of the system were increased to four by duplicating the two nominal inputs. Then, failure dynamics filters were appended to the plant at the inputs. Two types of failure dynamics were included. The first filter dynamics was chosen to represent an actuator dynamics with significantly reduced bandwidth, i.e., a low pass filter, as follows:

\[ F_1(s) = \frac{2\pi}{s + 2\pi} \]  

(25)

The second failure filter was chosen to be the complement of the first (in the lower frequencies) along with a roll-off at 10 Hz.

\[ F_2(s) = (1 - F_1(s)) \frac{20\pi}{s + 20\pi} \]  

(26)

It is interesting to note that the combination of the two filters gives the dynamics of a fully functional actuator with a roll-off at 10 Hz. Hence, these dynamics can serve to represent both soft and hard failures. Moreover, three distinct design criteria may be considered with this formulation. They are designs for soft failure only, hard failure only, and soft and hard failures. The frequency response coverage provided by the appended failure dynamics, in terms of gain attenuation and phase changes, for each design criteria is illustrated in Figure 4. As expected, the hard failure case (Figure 4(a)) allows for actuator gain variations between 0 and 1 with no variations in phase. The soft failure case does allow for phase variations as well as some gain variations. The combined case (Figure 4(c)) allows both gain and phase variations.

Let the columns of the expanded \( B \) matrix correspond to input no. 1 with \( F_1(s) \), input no. 1 with
is not maintained for most of the failure conditions. To ensure good performance on the nominal system, this performance that although the straight//2 control law has the best combined hard and soft failures. The results are sum-

MATLAB environment. The LMI conditions were solved using “SeDuMi”, a sparse convex solver for single-fault failures. The LMI problems were posed using “YALMIP”, which is an LMI parser for use in the MATLAB environment. The LMI conditions were formulated as a Lyapunov matrix in the multi-vertex LMI formulation. This conservatism is easily observed in Tables 1-3. The performance of the FS and convex-hull controllers are slightly worse than the H2 for the nominal plant (no failure). However, they are fully stable and maintain a good performance through different soft and hard failure scenarios. As mentioned before, the FS controller requires real-time measurement of the failure-state, and thus is not feasible for most applications. The fixed gain convex-hull control law has a higher bound than the FS control law, but the performance is similar (and in many cases even better) and it has the significant advantage of not requiring knowledge on the failure state of the system. These results are also illustrated graphically in Figures 5-7. Here, singular value plots of the transfer function from disturbance to performance output are provided for the three failure scenarios. A significant degradation in the first mode attenuation is observed in the straight H2 control, particularly for hard and combined failure modes. Also, both the FS and convex-hull controllers exhibit a loss of performance in the second mode for the hard and combined failure modes. This is the cost of ensuring robustness against total failure in any one actuator. It should be emphasized that these plots may only be used as a ways of observing trends in the frequency domain, and are not suitable to indicate closed-loop instabilities. Hence, closed-loop instabilities with the H2 controller, although there, cannot be seen in these plots.

Finally, a Monte Carlo analysis of the performance of these three controller were performed. A set of three analysis, one for each type of failure considered, were conducted. In each of these analysis, 500 points were randomly chosen in the convex hull formed by the vertex points in each design, and then the H2 norms were computed. The results of these analysis are summarized in Figure 8, wherein histograms of the H2 norms are illustrated for each of the three controllers and each of the failure cases. The range of variations for each controller is provided in the legends. In the combined failure scenario, the range of variations of the H2 norm with the straight H2 controller is 0.26 – 0.98, while that range with the convex-hull controller is 0.40 – 0.46. These results clearly demonstrate the effectiveness of the proposed fault-accommodating control technique.

Concluding Remarks
Control of flexible systems subject to degradation or total failure of actuators was considered. A Linear Matrix Inequality framework was developed to synthesize
a fixed-gain controller that had known $H_2$ norm performance bounds under a variety of input faults. These faults included soft failures, in the form of gain attenuation and phase changes, as well hard failures. The proposed approach was applied to the design of fault-tolerant control of a simple three degrees-of-freedom system. The benefits of the fault-tolerant design over conventional $H_2$ approach were clearly demonstrated. Finally, the proposed approach can easily be extended to deal with sensor failures/faults.

### References


Fig. 3  Schematic of the example spring-mass-damper system

Fig. 4  Frequency Response of single actuator (Nominal x's) under random failures (solid lines) for hard soft and the combined failure cases.
Fig. 5 Performance of open and closed-loop system under nominal and cases of full hard failure.

Fig. 6 Performance of open and closed-loop system under nominal and cases of full soft failure.
Fig. 7 Performance of open and closed-loop system under nominal and cases of full combined failure.

Fig. 8 Monti-Carlo style performance of random sampled systems under various failure conditions.