Design of Built-In Tests for Robust Active Fault Detection and Isolation of Discrete Faults in Uncertain Systems

William T. Hale[1], Kyle A. Palmer[1], Matthew D. Stuber[1], and George M. Bollas[1,*]

Abstract— **This work deals with the design of health maintenance tests for systems operating under uncertainty. Faults masked by uncertainty or uncertainty interpreted as a system fault often lead to subsequent safety and performance complications instantiated as false alarms, no fault founds, and non-detections. Here, a model-based active fault detection and isolation algorithm is employed in the form of a semi-infinite, worst-case scenario design program. The objective of this program is to maximize the fault detection and isolation capability at the worst-case realization of uncertainty, by manipulating the admissible system inputs. Fault detection and isolation are improved by increasing the distance between sensed outputs of the fault-free and faulty systems. The proposed method is demonstrated with application to the benchmark three-tank system with uncertain pipe flow coefficients, along with a faulty pump actuator and an unknown tank leak. The corresponding optimization problem is solved locally and globally using different worst-case design algorithms.**

I. INTRODUCTION

A. Built-In Test Design for Fault Detection and Isolation of Complex Systems

Health diagnostics in modern and complex cyber-physical systems is becoming increasingly challenging. Advanced and accurate system prognostics and diagnostics are crucial for system reliability and safety, especially in safety-critical systems, such as aircraft systems or chemical plants. The robustness of health checks employed during system maintenance depends on the method of fault detection and isolation (FDI) used. Significant research has been dedicated in the past couple decades on model-based and data-based methods for passive and active FDI [1]–[6]. Model-based methods of active FDI gained popularity, because they alleviate the high cost of equipment redundancy, while they leverage the increasing computation capacity of modern systems. Use of model-based active FDI methods in prognostics and diagnostics reduces the cost and increases the accuracy of maintenance by computationally "experimenting" with valid systems models, with the goal to manipulate admissible system inputs to reach optimal conditions for diagnosing faults. Therefore, active FDI methods can improve the robustness and accuracy of FDI in maintenance tests, in which system conditions can mask the fault (i.e., due to uncertainty) or uncertainty can be interpreted as a fault (i.e., false alarms) [7], [8].

In the automotive and aerospace industries, prognostics and diagnostics are commonly deployed through built-in tests (BITs). The term built-in test refers to system-integrated methods for FDI used in system health checks and maintenance tests. More specifically, initiated BITs are tests executed during maintenance and have relaxed performance requirements, allowing the admissible system inputs to be adjusted for improved FDI capabilities. Within this relaxed operating envelope, this work focuses on the design of optimal initiated BIT designs (i.e., optimal system conditions for BIT execution), which have the potential to improve system reliability and safety by alleviating the impacts of uncertainty and multiplicity of faults.

B. Application of Optimization and Uncertainty Analysis to Built-In Test Design

Research on optimization-based methods for FDI aims to improve the robustness and accuracy of the tests deploying it. [9]–[12]. Hale and Bollas [13] proposed an active FDI method that optimizes the system operating conditions to obtain unique system outputs for the isolation of several discrete faults, in the absence of uncertainty. However, accounting for uncertainty is a key component of robust FDI, especially for safety-critical system faults that require detection feasibility at all realizations of uncertainty. Mesbah et al. [14] studied a probabilistic approach to active FDI that optimized an input sequence for a three tank system under input and state constraints and improved fault detectability and isolability by separating the uncertain output distributions of various fault scenarios. Scott et al. [15] use a set-based approach to compute separating inputs (inputs that provide outputs unique to at most one fault for all uncertainties) that guarantee fault diagnosis and select the optimal separating input with minimum norm. Streif et al. [16] certified the robustness of active FDI by calculating an uncertain input signal that separates outputs in a finite number of steps, while also minimizing the number of outputs and measurements required for robustness to subsequently reduce costs. Palmer et al. [17] proposed a methodology that designs a BIT using the D-optimality criterion and accounts for uncertainties using a frequentist approach. The drawback of these methods is the requirement of knowing the probabilistic information of the uncertain inputs and parameters *a priori*.

C. Semi-Infinite Programming for Worst-Case Design of BIT

Interest in semi-infinite programming (SIP) has existed for decades in a wide range of research communities [18]. These problems involve the optimization of a desired objective,

*Corresponding author

[1]Department of Chemical & Biomolecular Engineering, University of Connecticut, 191 Auditorium Road, Unit 3222, Storrs, CT 06269, USA. {william.hale, kyle.palmer, matthew.stuber, george.bollas}@uconn.edu

based on a finite set of design variables and an infinite number of constraints dependent upon these design variables. As highlighted by Kettich and Kortanek [19], these problems are typically constructed into finite equivalents, which are then solved using conventional algorithms. A specific subset of SIPs for the optimization of systems under uncertainty is the worst-case approach [20]–[22]. This approach does not require probabilistic information *a priori*, as it uses only the domain knowledge of uncertainty. The worst-case approach is particularly useful for the robust FDI problem application discussed earlier, and specifically in determining design feasibility for safety-critical systems.

D. Contributions of This Work

In this work we apply a worst-case criterion to the design of tests for active FDI, targeting system health maintenance tests that can alleviate (or eliminate) common issues with false alarms, no faults found, and non-detections. In Section II, we present the proposed FDI problem formulation. In Section III we illustrate the application of this formulation to a benchmark three tank system and attempt to solve it locally and globally using algorithms developed by Asprey and Macchietto [20] and Stuber et al. [22], [23], respectively. We conclude by illustrating non-convexities in the worst-case FDI tests of (even) simple systems and highlight the significance of obtaining global feasible solutions.

II. MATHEMATICAL FORMULATION OF BIT DESIGN FOR ROBUST ACTIVE FDI

A. Model Definition

The proposed robust FDI method follows a similar formulation to [13], with minor simplifications. The steady-state algebraic equations describing the system are expressed as:

$$\mathbf{f}^{[f]}(\tilde{\mathbf{x}},\mathbf{u},\theta_p,\theta_u,\theta_f)=\mathbf{0}, \quad \forall f \in \{0,1,...,N_f\} \tag{1}$$

where the superscript $[f]$ (excluded from impacted variables for compactness) denotes the fault scenario studied, $\mathbf{f}^{[f]}$: $D_x \times D_u \times D_{\theta_p} \times D_{\theta_u} \times D_{\theta_f} \to \mathbb{R}^{N_x}$ is the set of continuously differentiable system of governing equations corresponding to $[f]$, $\tilde{\mathbf{x}} \in \tilde{X} \subset \mathbb{R}^{N_x}$ is the vector of system states, $\mathbf{u} \in U \subset \mathbb{R}^{N_u}$ is the vector of admissible system inputs, $\theta_p \in \Theta_p \subset \mathbb{R}^{N_{\theta_p}}$ is the vector of system design parameters augmented with all other model parameters, $\theta_u \in \Theta_u \subset \mathbb{R}^{N_{\theta_u}}$ is the vector of uncertain parameters, and $\theta_f \in \Theta_f \subset \mathbb{R}^{N_{\theta_f}}$ is the vector of parameters representing faults. The system outputs are expressed as:

$$\mathbf{y}^{[f]} = \bar{\mathbf{x}} + \mathbf{w}, \tag{2}$$

where $\mathbf{y}^{[f]} \in Y \subset \mathbb{R}^{N_y}$, is the vector of system outputs corresponding to $[f]$, $\bar{\mathbf{x}} \in \bar{X} \subseteq \tilde{X} \subset \mathbb{R}^{N_y}$ is the reduced or equivalent sized vector of measured system states, and $\mathbf{w} \in W \subset \mathbb{R}^{N_y}$, is the vector of measurement noise. A partial mapping is assumed in (1) for the functional relationship between the system outputs and the states. More traditional relationships of the system outputs with states, inputs, and parameters are feasible by augmenting (1).

B. Implicit SIP Formulation of Worst-Case BIT Design

The main goal of implementing model-based FDI methods in system health monitoring tests, such as BIT, is to be able to detect when faults occur in a system by observing and comparing the measured outputs to the outputs of the model. Once a fault is detected, a subsequent goal is to be able to accurately isolate the fault scenario that is present by matching the measured outputs of the system to the outputs of a fault model. Challenges arise when each fault scenario is not unique in its model outputs or when a fault is masked at the current operating condition due to control loops or uncertainty (in measurements, inputs, faults, and the system model) [14], [24]–[26]. For a "fully reliable" BIT, the test must fully detect and isolate all potential faults for any of the aforementioned uncertainties. A conservative BIT that is robust to all uncertainties is designed by analyzing the worst-case realization of uncertainty to determine if a feasible test exists that is capable of producing unique system outputs for every fault scenario. When designing a BIT, the following decision variables are often available to tune a test: the number of tests (sets of inputs); the duration of these tests; their dynamic responses; the frequency and type of sensors used; and the admissible system inputs. The worst-case BIT design can be formulated mathematically as a max-min problem, which in its simplest form uses only the admissible system inputs as manipulated variables at steady-state:

$$\begin{aligned} &\max_{\mathbf{u}\in U} \min_{\theta_u \in \Theta_u, \theta_f \in \Theta_f} G(\tilde{\mathbf{x}},\mathbf{u},\theta_p,\theta_u,\theta_f) \\ &\text{s.t. } \mathbf{f}(\tilde{\mathbf{x}},\mathbf{u},\theta_p,\theta_u,\theta_f) = \mathbf{0}, \end{aligned} \tag{3}$$

where $G : D_x \times D_u \times D_{\theta_p} \times D_{\theta_u} \times D_{\theta_f} \to \mathbb{R}$ is the continuously differentiable feasibility criterion that defines the quality of the BIT design and $\mathbf{f}(\tilde{\mathbf{x}},\mathbf{u},\theta_p,\theta_u,\theta_f) = (\mathbf{f}^{[1]},\mathbf{f}^{[2]},...,\mathbf{f}^{[N_f]})$ is the combined vector of equations for all fault scenarios from (1) with augmented variables.

With some mild assumptions from implicit function theory [22], if at least one $\tilde{\mathbf{x}}$ exists that satisfies (1) and (2), then it defines an implicit function of $(\mathbf{u},\theta_p,\theta_u,\theta_f)$, expressed as $\tilde{\mathbf{x}} = \mathbf{x}(\mathbf{u},\theta_p,\theta_u,\theta_f)$. Given the existence and uniqueness of the implicit function $\mathbf{x} : U \times \Theta_p \times \Theta_u \times \Theta_f \to X$, such that $\mathbf{f}(\mathbf{x}(\mathbf{u},\theta_p,\theta_u,\theta_f),\mathbf{u},\theta_p,\theta_u,\theta_f) = 0$, $\forall(\mathbf{u},\theta_p,\theta_u,\theta_f) \in U \times \Theta_p \times \Theta_u \times \Theta_f$ with $X \subset \tilde{X}$, the equality constraints of (3) can be eliminated to formulate an SIP below:

$$\begin{aligned} &\min_{\mathbf{u}\in U,\ \eta \in H} -\eta \\ &\text{s.t. } g(\mathbf{x}(\mathbf{u},\theta_p,\theta_u,\theta_f),\mathbf{u},\theta_p,\theta_u,\theta_f,\eta) \leq 0 \\ &\forall\ (\theta_u,\theta_f) \in \Theta_u \times \Theta_f, \end{aligned} \tag{4}$$

where $\eta \in H \subset \mathbb{R}$ is an auxiliary variable introduced for the SIP formulation and g is a continuously differentiable inequality constraint formulated as:

$$\begin{aligned} &g(\mathbf{x}(\mathbf{u},\theta_p,\theta_u,\theta_f),\mathbf{u},\theta_p,\theta_u,\theta_f,\eta) = \\ &\eta - G(\mathbf{x}(\mathbf{u},\theta_p,\theta_u,\theta_f),\mathbf{u},\theta_p,\theta_u,\theta_f). \end{aligned} \tag{5}$$

C. Global Solutions to Implicit SIPs

The program (4) has a finite number of variables yet an infinite number of constraints due to g, which is realized

Algorithm 1 SIP Max-Min Algorithm

```
Require: $\theta_u^{[1]} \in \Theta_u, \theta_f^{[1]} \in \Theta_f$
K ← 1   ($K \leftarrow 1$)
while $\hat{\eta}^{[K]} < \eta^{[K]} \wedge K \leq K_{max}$ do
    $(\eta^{[K]}, \mathbf{u}^{[K]}) \leftarrow \min_{\mathbf{u} \in U,\ \eta \in H} -\eta$
    s.t. $\eta - G(\mathbf{x}(\mathbf{u}, \theta_p, \theta_u^{[k]}, \theta_f^{[k]}), \mathbf{u}, \theta_p, \theta_u^{[k]}, \theta_f^{[k]}) \leq 0,$
    $\forall k \in \{1, 2, ..., K\}$
    $(\hat{\eta}^{[K]}, \theta_u^{[K+1]}, \theta_f^{[K+1]}) \leftarrow$
        $\min_{\theta_u \in \Theta_u, \theta_f \in \Theta_f} G(\mathbf{x}(\mathbf{u}^{[K]}, \theta_p, \theta_u, \theta_f), \mathbf{u}^{[K]}, \theta_p, \theta_u, \theta_f)$
    $K \leftarrow K + 1$
end
$(\mathbf{u}^{opt}, \theta_u^{opt}, \theta_f^{opt}) \leftarrow (\mathbf{u}^{[K-1]}, \theta_u^{[K]}, \theta_f^{[K]})$
```

across the entirety of the parameterized uncertainty and fault domains. The infinite nature of (4) differs from standard NLPs and makes it quite difficult to solve. A similar type of problem was proven to be locally solvable by Asprey and Macchietto [20] using Alg. 1. This algorithm likely requires an assumption on convexity, as the objective function of [20] is convex in nature [27], and this assumption is tested in this work to explore the algorithm's finite convergence. Alg. 1 holds for systems with bounded uncertainties, which is often the case for engineered systems.

Alg. 1 solves (4) by first taking an initial set of values for the uncertain parameters and finding the optimal BIT design at the given uncertainty. It then uses the optimal BIT design to try and find a new set of uncertain parameter values that performs worse than the initial set, adding this set to an overall uncertainty set comprised of the previous parameter sets. At each iteration, the optimal BIT must satisfy its constraints for the current set of uncertain parameters and all other parameter sets in the overall uncertainty set. The algorithm terminates at an optimal worst-case BIT design when no new set of uncertain parameters that performs worse than all previous sets can be found. If the algorithm iterates to its maximum K_{max} and no feasible solution has been found, then the system design space, uncertainties, and constraints should be reconsidered.

Although the assumption on convexity made for Alg. 1 seems to be sufficient for the application presented in Sec. III, global methods are required to guarantee feasibility in cases when this assumption fails. Global methods address the issue of local solutions caused by non-convexities in SIPs. Falk and Hoffman [28] extend upon Blankenship and Falk's [29] cutting-plane algorithm for solving nonlinear explicit SIPs to examine large classes of non-convex functions. Mitsos [30] improved upon the Blankenship and Falk [29] algorithm by utilizing an upper-bounding procedure that perturbs the right-hand side of the semi-infinite constraint in (4), guaranteeing the generation of SIP-feasible points in a finite manner for continuous NLPs that contain Slater points. Stuber and Barton [22] adapted the work of Mitsos [30] to allow for its application to implicit SIPs. The method of [22] is used here for the worst-case-scenario design of FDI tests in systems under uncertainty. The results of Alg. 1 and the global method presented in [22] are presented at the end of Section III.

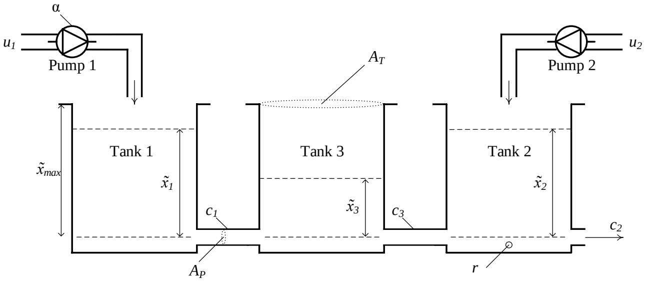

Fig. 1. Three tank system model architecture from Mesbah et al. [14] with labeled system states $\tilde{\mathbf{x}} = [\tilde{x}_1, \tilde{x}_2, \tilde{x}_3]$, inputs $\mathbf{u} = [u_1, u_2]$, design parameters $\theta_p = [A_T, A_P]$, uncertain parameters $\theta_u = [c_1, c_2, c_3]$, and fault parameters $\theta_f = [\alpha, r]$.

III. APPLICATION TO A THREE TANK SYSTEM

A. Three Tank System Model Equations

The example system modeled and studied in this work is the benchmark three tank system described in [14] with $N_u = 2$, $N_{\theta_u} = 3$, $N_{\theta_f} = 2$, and $N_y = 3$. Fig. 1 shows the corresponding three tank system architecture, component labels, and variables. Tanks 1, 2, and 3 are cylindrical with equivalent cross-sectional area $A_T = 0.0154$ m^2 and height $\tilde{x}_{max} = 0.75$ m. The admissible system inputs are the assigned liquid flow rates of Pumps 1 and 2: u_1 and u_2 $(m^3 s^{-1})$. The pipes connecting and exiting Tanks 1, 2, and 3 have equal cross-sectional area $A_p = 0.00005$ m^2. The liquid flow rates exiting Tanks 1, 2, and 3 are characterized by their respective non-dimensional flow coefficients: c_1, c_2, and c_3. The system state $\tilde{x}_i^{[f]}$ (m) corresponds to liquid height of Tank i from the fault scenario model f ($f = 0$ for the fault-free system). Two uncertain fault scenarios are studied for robust detection and isolation: a degradation to Pump 1 ($f = 1$) and a leak in Tank 2 ($f = 2$). The degradation of Pump 1 is characterized by the non-dimensional flow coefficient α, which impacts the flow rate of the liquid supplied to Tank 1. The leak in Tank 2 is circular and is characterized by the radius r (m).

The assigned liquid flow rates of Pumps 1 and 2, u_1 and u_2, will be considered the system admissible inputs $\mathbf{u} = (u_1, u_2)$. The pump degradation coefficient α and leak radius r are considered parameters representing faults, $\theta_f = (\alpha, r)$ and the flow coefficients c_1, c_2 and c_3, are considered as uncertain parameters, $\theta_u = (c_1, c_2, c_3)$. The liquid heights of Tanks 1, 2, and 3 for each fault scenario are the system states, $\tilde{\mathbf{x}} = (\tilde{x}_1^{[0]}, \tilde{x}_2^{[0]}, \tilde{x}_3^{[0]}, \tilde{x}_1^{[1]}, \tilde{x}_2^{[1]}, \tilde{x}_3^{[1]}, \tilde{x}_1^{[2]}, \tilde{x}_2^{[2]}, \tilde{x}_3^{[2]})$. Perfectly measured ($\mathbf{w} = \mathbf{0}$) liquid heights of tanks 1, 2, and 3 are the system outputs, $\mathbf{y} = \tilde{\mathbf{x}}$.

The combined set of steady-state system model equations developed from the conservation of mass and Torricelli's law for each fault scenario is shown below:

$$\mathbf{f}(\tilde{\mathbf{x}},\mathbf{u},\theta_p,\theta_u,\theta_f) = (\mathbf{f}^{[0]},\mathbf{f}^{[1]},\mathbf{f}^{[2]}) = \mathbf{0} =$$
$$\begin{pmatrix} -c_1 A_P \tanh(k\Delta\tilde{x}_{13}^{[0]})\sqrt{2g\sqrt{(\Delta\tilde{x}_{13}^{[0]})^2}} + u_1 \\ -c_3 A_P \tanh(k\Delta\tilde{x}_{23}^{[0]})\sqrt{2g\sqrt{(\Delta\tilde{x}_{23}^{[0]})^2}} - c_2 A_P\sqrt{2g\tilde{x}_2^{[0]}} + u_2 \\ c_1 A_P \tanh(k\Delta\tilde{x}_{13}^{[0]})\sqrt{2g\sqrt{(\Delta\tilde{x}_{13}^{[0]})^2}} - c_3 A_P \tanh(k\Delta\tilde{x}_{32}^{[0]})\sqrt{2g\sqrt{(\Delta\tilde{x}_{32}^{[0]})^2}} \\ -c_1 A_P \tanh(k\Delta\tilde{x}_{13}^{[1]})\sqrt{2g\sqrt{(\Delta\tilde{x}_{13}^{[1]})^2}} + u_1 + (\alpha - 1)u_1 \\ -c_3 A_P \tanh(k\Delta\tilde{x}_{23}^{[1]})\sqrt{2g\sqrt{(\Delta\tilde{x}_{23}^{[1]})^2}} - c_2 A_P\sqrt{2g\tilde{x}_2^{[1]}} + u_2 \\ c_1 A_P \tanh(k\Delta\tilde{x}_{13}^{[1]})\sqrt{2g\sqrt{(\Delta\tilde{x}_{13}^{[1]})^2}} - c_3 A_P \tanh(k\Delta\tilde{x}_{32}^{[1]})\sqrt{2g\sqrt{(\Delta\tilde{x}_{32}^{[1]})^2}} \\ -c_1 A_P \tanh(k\Delta\tilde{x}_{13}^{[2]})\sqrt{2g\sqrt{(\Delta\tilde{x}_{13}^{[2]})^2}} + u_1 \\ -c_3 A_P \tanh(k\Delta\tilde{x}_{23}^{[2]})\sqrt{2g\sqrt{(\Delta\tilde{x}_{23}^{[2]})^2}} - c_2 A_P\sqrt{2g\tilde{x}_2^{[2]}} - c_2\pi r^2\sqrt{2g\tilde{x}_2^{[2]}} + u_2 \\ c_1 A_P \tanh(k\Delta\tilde{x}_{13}^{[2]})\sqrt{2g\sqrt{(\Delta\tilde{x}_{13}^{[2]})^2}} - c_3 A_P \tanh(k\Delta\tilde{x}_{32}^{[2]})\sqrt{2g\sqrt{(\Delta\tilde{x}_{32}^{[2]})^2}} \end{pmatrix}, \qquad (6)$$

where lines 1-3 correspond to $\mathbf{f}^{[0]}$, lines 4-6 correspond to $\mathbf{f}^{[1]}$, lines 7-9 correspond to $\mathbf{f}^{[2]}$, $\Delta\tilde{x}_{ij}^{[f]} \equiv \tilde{x}_i^{[f]} - \tilde{x}_j^{[f]}$, and $\tanh(k)$ is an approximation of the signum function used to satisfy the differentiability assumption.

B. Objective Function and SIP Formulation of Worst-Case BIT Design

The objective function G used in this work for BIT design is the separation between fault-free and faulty system outputs. This is defined mathematically below for all fault scenarios $N_f = 2$:

$$G(\mathbf{x}(\mathbf{u},\theta_p,\theta_u,\theta_f),\mathbf{u},\theta_p,\theta_u,\theta_f) = \\ -\eta_{feas} + \sum_{i=1}^{N_y}\sum_{f=0}^{N_f-1}\sum_{g=f+1}^{N_f}(y_i^{[f]} - y_i^{[g]})^2, \qquad (7)$$

and results in the following SIP formulation updated with the objective (7):

$$\min_{\mathbf{u}\in U,\ \eta\in H} -\eta$$
$$\text{s.t. } \eta - \sum_{i=1}^{N_y}\sum_{f=0}^{N_f-1}\sum_{g=f+1}^{N_f}(y_i^{[f]} - y_i^{[g]})^2 + \eta_{feas} \le 0 \qquad (8)$$
$$\forall\ (\theta_u,\theta_f) \in \Theta_u \times \Theta_f,$$

where $\eta_{feas} \in H^{feas} \subset \mathbb{R}$ is the FDI performance parameter specifying a minimum separation constraint. An $\eta^{opt} < 0$ implies no feasible worst-case BIT design exists that is capable of producing the desired separation η_{feas} for all realizations of uncertainty in $\Theta_u \times \Theta_f$. However, $\eta^{opt} \ge 0$ means there is a feasible worst-case BIT design that satisfies η_{feas}.

For (8), the state interval is $\tilde{X} = [0, 0.75]^9$, the BIT design interval is $U = [10^{-5}, 10^{-4}]^2$, the uncertainty parameter interval is $\Theta_u = [0.85, 1.15] \times [0.65, 0.95] \times [0.85, 1.15]$, the fault parameter interval is $\Theta_f = [0.54, 0.66] \times [0.0005, 0.005]$, the SIP auxiliary variable interval is $H = [-10, 10]$, and the FDI performance parameter is $\eta_{feas} = 0.1$. These intervals were derived from the probabilistic information of Table I provided by [14] and were assumed to enclose the implicit function $\mathbf{x} : U \times \Theta_p \times \Theta_u \times \Theta_f \to X$, such that $\mathbf{f}(\mathbf{x}(\mathbf{u},\theta_p,\theta_u,\theta_f),\mathbf{u},\theta_p,\theta_u,\theta_f) = 0,\ \forall(\mathbf{u},\theta_p,\theta_u,\theta_f) \in U \times \Theta_p \times \Theta_u \times \Theta_f$.

TABLE I

DESCRIPTION OF THE FAULTS $\theta_f = [\alpha, r]$ AND UNCERTAINTIES $\theta_u = [c_1, c_2, c_3]$ STUDIED IN THE THREE TANK SYSTEM OF FIG. 1 AND THEIR NORMALLY DISTRIBUTED $\mathcal{N}(\mu, \sigma^2)$ RANDOM PARAMETER VALUES WITH MEAN μ AND VARIANCE σ^2 [14].

Faults and Uncertainties	Parameters	Uncertainty Distribution
Pump 1 Degradation Coefficient	$\theta_{f,1} = \alpha$	$\mathcal{N}(0.6, 4 * 10^{-4})$
Tank 2 Leak radius	$\theta_{f,2} = r$	$\mathcal{N}(2 * 10^{-2}, 1 * 10^{-6})$
Tank 1 Flow Coefficient	$\theta_{u,1} = c_1$	$\mathcal{N}(1.0, 2.5 * 10^{-3})$
Tank 2 Flow Coefficient	$\theta_{u,2} = c_2$	$\mathcal{N}(0.8, 2.5 * 10^{-3})$
Tank 3 Flow Coefficient	$\theta_{u,3} = c_3$	$\mathcal{N}(1.0, 2.5 * 10^{-3})$

TABLE II

BOUNDS AND SOLUTION TO (8) FOR THE THREE TANK SYSTEM BIT DESIGN AT THE WORST-CASE REALIZATION OF UNCERTAINTY.

Inputs and Parameters	Min	Nominal	Optimal	Max
u_1 $(m^3 s^{-1} * 10^{-4})$	0.10	0.41	0.80	1.00
u_2 $(m^3 s^{-1} * 10^{-4})$	0.10	0.41	0.10	1.00
$\theta_{f,1}$ $(-)$	0.54	0.66	0.66	0.66
$\theta_{f,2}$ (m)	0.00	0.0014	0.0022	0.005
$\theta_{u,1}$ $(-)$	0.85	1.15	1.15	1.15
$\theta_{u,2}$ $(-)$	0.65	0.95	0.95	0.95
$\theta_{u,3}$ $(-)$	0.85	1.15	1.15	1.15

The three tank system model equations (6) used in solving this SIP were programed in MATLAB® [31], where a robust BIT design solution to (8) was found using the MATLAB® OPTI Toolbox with the Mesh Adaptive Direct Search algorithm and Alg. 1. Table II provides the nominal and optimal inputs and their corresponding worst-case uncertain parameters, along with the interval bounds of each variable. The upper and lower bounds of the parameter intervals were calculated from the three sigma values of the distributions presented in Table I.

Fig. 2 shows the dynamically simulated outputs of the three tank system at the nominal and optimal conditions of Table II. The dynamic system model equations are $A_t\dot{\tilde{\mathbf{x}}} = \mathbf{f}(\tilde{\mathbf{x}},\mathbf{u},\theta_p,\theta_u,\theta_f)$, where $\dot{\tilde{\mathbf{x}}} \in \tilde{X} \subset \mathbb{R}^{N_x}$ is the vector of state variable time derivatives. These dynamic outputs are equivalent to the outputs calculated from solving (6) once steady-state is achieved. The objective functions calculated at these conditions were $G^{nom} = 0.018261$ and $G^{opt} = 0.1126$. This objective calculated the distance between the outputs of the different fault scenarios and was evaluated at the respective worst-case realization of uncertainty for the nominal and optimal conditions. In the nominal case, there is little to no separation of the three outputs for the three different fault scenarios. At these nominal system conditions, the uncertainty causes the fault scenarios to be indistinguishable from the fault-free system resulting in non-detections during operation or no fault found occurrences during maintenance. In the optimal case, all three outputs of the three fault scenarios have adequate separation which is beneficial for detection and isolation purposes. The inputs of the optimal BIT design are selected to maximize the FDI test performance, while ensuring the system tank heights are valid (within their intervals, i.e., dotted black lines in Fig. 2) for every possible realization of uncertainty. This is the main reason why the inputs did not reach their respective interval bounds. Expanding the system tank height intervals through adjustments to the physical system design would likely cause the inputs to reach their respective upper or lower interval bounds and significantly improve the BIT performance.

Fig. 3 is descriptive of this conclusion, showing the objective function over the input set U for the worst-case realization of uncertainty without consideration of state constraints. The greatest objective function value lies at the upper bounds of inputs 1 and 2. However, it is important to mention that this result is not necessarily the solution to (8). By following the max-min inequality, the result shown acts as an upper bound to the feasible region of (8). The actual objective function in the feasible region of (8) will be less than or equal to what is shown in Fig. 3. Looking simply at this upper bound, the objective function seems to be convex, verifying the assumption made on convexity. However, it is still of interest to use global methods such as those described at the end of Section II to observe whether or not an improvement in BIT design can be found.

The three tank system model equations (6) and worst-case BIT design SIP (8) were also formulated in the GAMS modeling environment [32]. In GAMS, the global algorithm adapted from the work of Mitsos [30] and presented by Stuber and Barton in [22] was used to find the global optimum of (8) using the Branch-And-Reduce Optimization Navigator, BARON [33]. It was seen that Alg. 1 could only converge to the global solution using multiple shooting methods for the constrained (by output constraints) feasible set of inputs. Ongoing work focuses on the impact of local solutions on system safety, depending on the criticality of faults. This analysis will determine the need for application of global optimization techniques in systems of considerably larger scale, than that of the three tank benchmark.

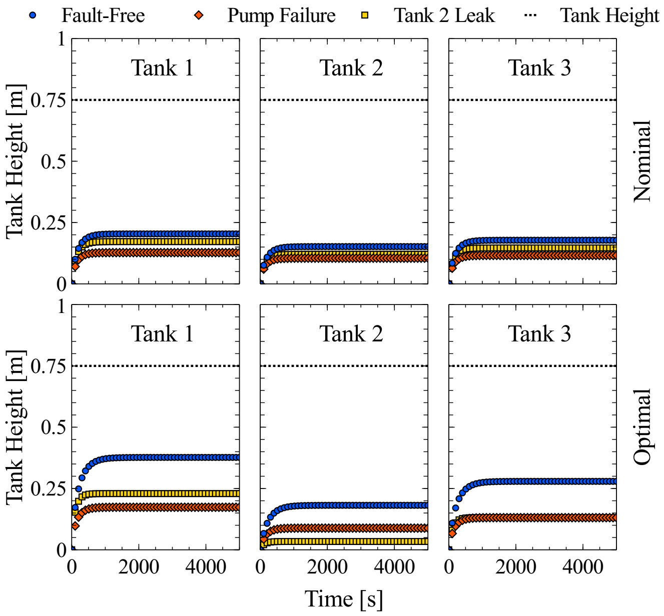

Fig. 2. Three tank system heights of the fault-free and two fault cases studied at the worst-case realization of uncertainties shown in Table II for the nominal inputs $\mathbf{u}^{nom} = [0.41*10^{-4}, 0.41*10^{-4}]$ and optimal inputs $\mathbf{u}^{opt} = [0.80*10^{-4}, 0.10*10^{-4}]$.

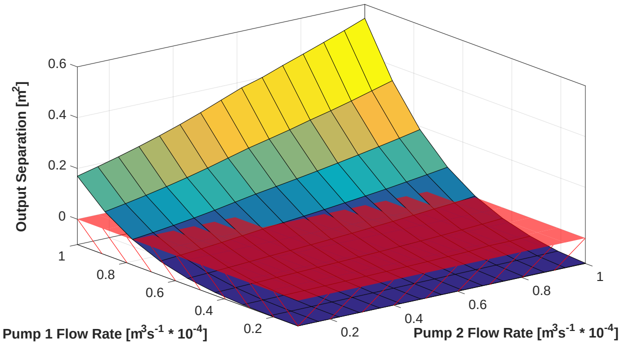

Fig. 3. The upper bound of program (8) showing the objective function (7), η^{opt}, calculated for the worst-case realization of uncertainty without state constraint consideration. The red xy-plane at z=0 displays the feasible region of FDI performance, above which $\eta^{opt} \geq \eta_{feas}$, signifying a satisfactory worst-case BIT design.

IV. CONCLUSIONS AND FUTURE WORK

In this work, a method for developing robust maintenance tests on the basis of active FDI and worst-case design was presented. A semi-infinite program with the admissible system inputs as the manipulated variables was formulated to design robust maintenance tests for the worst-case realization of uncertainty. This problem was attempted to be solved locally using the algorithm presented by Asprey and Macchietto [20] and globally using a cutting plane algorithm presented by Stuber et al. [22]. The method and programs developed were applied on the three tank benchmark system. This example system is interesting for its nonconvex objective function. The optimal FDI tests designed were shown capable of distinguishing between a fault-free system and two separate fault scenarios, which was not feasible with a nominal FDI test design. Moreover, the nonconvexity of the objective function was shown to lead to local minima, which can lead to state constraint violations or non-decisive tests. Future work includes the utilization of dynamic system information in the objective function and state constraints (which was on a concern for the simple three tank system), false alarm rate analysis, and analysis of the sensor selection and the impact of variable levels of noise on maintenance test accuracy.

ACKNOWLEDGMENT

This project was sponsored by the UTC Institute for Advanced Systems Engineering (UTC-IASE) of the University of Connecticut and the United Technologies Corporation. Any opinions expressed herein are those of the authors and do not represent those of the sponsor. The authors would also like to thank Alexander Mitsos for providing access to

the global SIP algorithm within the GAMS environment and Matthew Wilhelm for the aid in global optimization.

References

[1] J. I. E. Chen, "Robust residual generation for model-based fault diagnosis of dynamic systems," Ph.D. dissertation, University of York, 1995.

[2] R. Isermann, "Model-based fault-detection and diagnosis status and applications," *Annual Reviews in Control*, vol. 29, no. 1, pp. 71–85, 2005.

[3] 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, 2010.

[4] J. Marzat, H. Piet-Lahanier, F. Damongeot, and E. Walter, "Model-based fault diagnosis for aerospace systems: a survey," *Proceedings of the Institution of Mechanical Engineers, Part G: Journal of Aerospace Engineering*, vol. 226, no. 10, pp. 1329–1360, 2012.

[5] A. Fekih, "Fault diagnosis and fault tolerant control design for aerospace systems: A bibliographical review," in *Proceedings of the American Control Conference*, 2014, pp. 1286–1291.

[6] A. Zolghadri, "Advanced model-based fdir techniques for aerospace systems: Today challenges and opportunities," *Progress in Aerospace Sciences*, vol. 53, pp. 18–29, 2012.

[7] M. Šimandl and I. Punčochář, "Active fault detection and control: Unified formulation and optimal design," *Automatica*, vol. 45, no. 9, pp. 2052–2059, 2009.

[8] H. Niemann, "Fault tolerant control based on active fault diagnosis," in *Proceedings of the American Control Conference*, vol. 3, 2005, pp. 2224–2229.

[9] K.-K. K. Kim, D. M. Raimondo, and R. D. Braatz, "Optimum input design for fault detection and diagnosis: Model-based prediction and statistical distance measures," in *Proceedings of the 2013 European Control Conference*, 2013, pp. 1940–1945.

[10] S. Yin, H. Luo, and S. X. Ding, "Real-time implementation of fault-tolerant control systems with performance optimization," *IEEE Transactions on Industrial Electronics*, vol. 61, no. 5, pp. 2402–2411, 2014.

[11] A. Rosich, R. Sarrate, V. Puig, and T. Escobet, "Efficient optimal sensor placement for model-based fdi using an incremental algorithm," in *Proceedings 46th IEEE Conference on Decision and Control*, 2007, pp. 2590–2595.

[12] D. Henry and A. Zolghadri, "Design of fault diagnosis filters: A multi-objective approach," *Journal of the Franklin Institute*, vol. 342, no. 4, pp. 421–446, 2005.

[13] W. T. Hale and G. M. Bollas, "Design of Built-In Tests for Active Fault Detection and Isolation of Discrete Faults," *IEEE Access*, 2018. In Review.

[14] A. Mesbah, S. Streif, R. Findeisen, and R. D. Braatz, "Active fault diagnosis for nonlinear systems with probabilistic uncertainties," *IFAC Proceedings Volumes*, vol. 47, no. 3, pp. 7079–7084, 2014.

[15] J. K. Scott, R. Findeisen, R. D. Braatz, and D. M. Raimondo, "Design of active inputs for set-based fault diagnosis," in *Proceedings of the American Control Conference*, 2013, pp. 3561–3566.

[16] S. Streif, D. Hast, R. D. Braatz, and R. Findeisen, "Certifying robustness of separating inputs and outputs in active fault diagnosis for uncertain nonlinear systems," *IFAC Proceedings Volumes*, vol. 46, no. 32, pp. 837–842, 2013, 10th IFAC International Symposium on Dynamics and Control of Process Systems.

[17] K. A. Palmer, W. T. Hale, K. D. Such, B. R. Shea, and G. M. Bollas, "Optimal design of tests for heat exchanger fouling identification," *Applied Thermal Engineering*, vol. 95, pp. 382–393, 2016.

[18] C. A. Floudas and C. E. Gounaris, "A review of recent advances in global optimization," *Journal of Global Optimization*, vol. 45, pp. 3–38, 2009.

[19] R. Hettich and K. O. Kortanek, "Semi-infinite programming: Theory, methods, and applications," *SIAM Review*, vol. 35, no. 3, pp. 380–429, 1993.

[20] S. Asprey and S. Macchietto, "Designing robust optimal dynamic experiments," *Journal of Process Control*, vol. 12, no. 4, pp. 545–556, 2002.

[21] C. R. Rojas, J. S. Welsh, G. C. Goodwin, and A. Feuer, "Robust optimal experiment design for system identification," *Automatica*, vol. 43, no. 6, pp. 993–1008, 2007.

[22] M. D. Stuber and P. I. Barton, "Semi-infinite optimization with implicit functions," *Industrial & Engineering Chemistry Research*, vol. 54, pp. 307–317, 2015.

[23] M. D. Stuber, A. Wechsung, A. Sundaramoorthy, and P. I. Barton, "Worst-case design of subsea production facilities using semi-infinite programming," *AIChE Journal*, vol. 60, no. 7, pp. 2513–2524, 2014.

[24] S. Khan, P. Phillips, I. Jennions, and C. Hockley, "No fault found events in maintenance engineering part 1: Current trends, implications and organizational practices," *Reliability Engineering & System Safety*, vol. 123, pp. 183–195, 2014.

[25] S. Khan, P. Phillips, C. Hockley, and I. Jennions, "No fault found events in maintenance engineering part 2: Root causes, technical developments and future research," *Reliability Engineering & System Safety*, vol. 123, pp. 196 – 208, 2014.

[26] P. Söderholm, "A system view of the no fault found (nff) phenomenon," *Reliability Engineering & System Safety*, vol. 92, pp. 1–14, 2007.

[27] A. DeCock, M. Gevers, and J. Schoukens, "D-optimal input design for nonlinear fir-type systems: A dispersion-based approach," *Automatica*, vol. 73, pp. 88–100, 2016.

[28] J. E. Falk and K. Hoffman, "A nonconvex max-min problem," *Naval Research Logistics Quarterly*, vol. 24, no. 3, pp. 441–450, 1977.

[29] J. W. Blankenship and J. E. Falk, "Infinitely constrained optimization problems," *Journal of Optimization Theory and Applications*, vol. 19, no. 2, pp. 261–281, 1976.

[30] A. Mitsos, "Global optimization of semi-infinite programs via restriction of the right-hand side," *Optimization*, vol. 60, no. 10-11, pp. 1291–1308, 2011.

[31] T. M. Inc., "Matlab," Natick, MA, 2017. [Online]. Available: https://www.mathworks.com/

[32] G. D. Corporation, "General Algebraic Modeling System (GAMS) Release 24.2.1," Washington, DC, USA, 2013. [Online]. Available: http://www.gams.com/

[33] M. Tawarmalani and N. V. Sahinidis, "A polyhedral branch-and-cut approach to global optimization," *Mathematical Programming*, vol. 103, no. 2, pp. 225–249, 2005.