Computers and Chemical Engineering 126 (2019) 218–230

Contents lists available at ScienceDirect

Computers and Chemical Engineering

journal homepage: www.elsevier.com/locate/compchemeng

Semi-infinite programming for global guarantees of robust fault detection and isolation in safety-critical systems

William T. Hale, Matthew E. Wilhelm, Kyle A. Palmer, Matthew D. Stuber*, George M. Bollas*

Department of Chemical & Biomolecular Engineering, University of Connecticut, 191 Auditorium Road, Unit 3222, Storrs, CT 06269, USA

ARTICLE INFO

Article history:
Received 15 February 2019
Revised 25 March 2019
Accepted 8 April 2019
Available online 11 April 2019

Keywords:
Fault detection and isolation
Global optimization
Robustness
Semi-infinite programs
Uncertain safety-critical systems
Worst-case design

ABSTRACT

The increasing uncertainty due to advances in modern systems has negatively impacted system health and safety. System health and safety problems associated with uncertainty can be attributed to (1) inadequate system design, (2) ill-suited controller and operating envelope, and (3) lack of robustness in system diagnostics. The latter issue (3) is the main focus of this paper. This work presents an algorithm for the design of active fault detection and isolation (FDI) tests that provide rigorous guarantees of robustness in safety-critical systems. A semi-infinite program with implicit functions embedded is formulated with the objective of maximizing FDI effectiveness at the worst-case realization of uncertainty by manipulating admissible system inputs, while taking into account system safety constraints. This problem is solved locally and globally illustrating deficiencies in the performance of FDI tests designed for the mean values of anticipated uncertainty. The resulting solution is an optimally performing fault diagnostic test that guarantees system safety over the entire domain of uncertainty. This is illustrated using a benchmark three-tank system and further analyzed through Monte Carlo simulation and *k*-NN classification.

1. Introduction

The scientific challenge of satisfying the strict requirements associated with safety-critical systems continues to grow as systems advance and increase in complexity, introducing additional uncertainty in boundaries, parameters, and faults. The added uncertainty from sources such as manufacturing defects and environmental disturbances negatively impacts system performance, reliability, and most importantly safety. Correspondingly, the accuracy of system fault diagnostics has also suffered from uncertainty, commonly due to model inaccuracies. The occurrence of faults and their missed detection due to uncertainty is problematic for safety-critical systems with rigid safety requirements. It is important for safety-critical systems with hazardous or fatal implications of occurring faults to be capable of detecting faults at low rates of false alarms, missed detections, and subsequent no fault found (NFF) events. da Silva et al. (2012) highlighted several sensor fault scenarios from the aerospace industry that have led to loss of mission or life. Saha and Sadi (2012) described the catastrophic consequences of safety violations in nuclear power plants, heart pace makers, and spacecraft, all of which motivate the need for safety-critical system dependability. Therefore, significant research effort has been made in recent years to improve the resiliency of safety-critical systems to faults and uncertainty (Kim et al., 2010; Ossmann, 2014; Wisniewski et al., 2013). However, there is still room for improvement in the field of system fault diagnostics, especially in terms of robustness.

The robustness of fault diagnostics, in particular the system health checks employed during maintenance, is highly dependent on the method of fault detection and isolation (FDI) used and its accuracy amid uncertainty. Therefore, much effort is focused on the formal design of fault diagnostics to improve FDI capability in terms of performance, reliability, and safety. This effort has led to the field of FDI garnering significant research attention over the past couple decades (Fekih, 2014; Hwang et al., 2010). Methods of FDI can be implemented in either a passive or active manner. Passive FDI methods are carried out during real time operation and detect irregularities or anomalies that occur through comparison with a predicted or anticipated behavior. However, the robustness of these methods depends on the system operating conditions as well as the fault severity and complexity (Ashari et al., 2012). A major concern regarding today's systems are intermittent faults that are only present at specific moments of an operating envelope. One of the benefits of active FDI methods

* Corresponding authors.
E-mail addresses: william.hale@uconn.edu (W.T. Hale), matthew.wilhem@uconn.edu (M.E. Wilhelm), kyle.palmer@uconn.edu (K.A. Palmer), matthew.stuber@uconn.edu (M.D. Stuber), george.bollas@uconn.edu (G.M. Bollas).

https://doi.org/10.1016/j.compchemeng.2019.04.007
0098-1354/

is that they overcome this issue by re-configuring the system into "optimal" state sequences or state trajectories that improve the detection and isolation of faults. Furthermore, model-based methods of active FDI have increased in popularity due to the fact they leverage the increasing computational capacity of modern systems, while also alleviating the high costs of handling faults with duplicate components/systems (Ashari et al., 2012; Niemann, 2006). Finally, model-based active FDI methods can be leveraged to improve the robustness of fault diagnostics during maintenance, where system conditions can mask the fault(s) present (i.e., no fault founds) or lead to misinterpretation of uncertainty as a fault (i.e., false alarms) (Šimandl and Punčochář, 2009). No fault found events arise when a definitive conclusion on system health cannot be made during maintenance (i.e., no fault is detected and/or isolated), despite an alarm being triggered during operation. This has been attributed to incorrect and inaccurate system fault diagnostics, more specifically the inability to replicate the conditions which triggered the alarm (Khan et al., 2014a; 2014b).

System diagnostic tests are typically carried out in the automotive and aerospace industries through built-in tests (BITs), which refer to system-integrated methods of FDI executed during operation and maintenance for system health checks. Of those, the so-called initiated BITs (IBITs) are tests specifically executed during maintenance as active FDI tests and as a result have relaxed system performance requirements. Relaxation of the normal operating constraints during IBITs allows for more impactful manipulation of admissible system inputs to improve FDI capabilities. Khan et al. (2014a,b) cite a need for improving FDI, specifically BIT, to address issues associated with uncertainty. The selection of an IBIT design can significantly impact the detection and isolation of faults, separate them from system uncertainty, and consequently improve maintenance costs, system reliability and safety (Venkatasubramanian et al., 2003). One powerful approach to IBIT design builds on the application of optimization techniques that manipulate system admissible inputs (Palmer and Bollas, 2018; 2019; Palmer et al., 2018). In previous work, Hale and Bollas (2018) mathematically formulated an active FDI method for obtaining unique system outputs that detect and isolate several faults by optimizing system operating conditions (i.e., admissible system inputs). However, the majority of prior work assumes the system is free of uncertainty or operating at mean anticipated values for uncertainty in system inputs, parameters, or boundaries. For safety-critical systems, a method is needed that accounts for all realizations of uncertainty, so that stringent safety requirements can be accounted for and formally addressed (e.g., zero allowed missed detections).

The task of designing robust FDI methods is often met with inaccurate system data, unknown environmental factors, limitations in system and external resources, and other sources of uncertainty that need to be accounted for. Previously Hale et al. (2018), we illustrated preliminary analyses of the impact of uncertainty on FDI. This builds upon the work by Mesbah et al. (2014), who take a probabilistic approach to active FDI and developed an optimal input sequence for a three-tank system, subject to input and state constraints, that separates the uncertain output probability distributions of different fault scenarios. Mesbah et al. addressed computational complexity by reducing the model equations to polynomial chaos expansions, and optimized the Hellinger distance, or distributional overlap, obtained from running Monte Carlo simulations at each iteration. Scott et al. (2013) developed a set-based approach to computing minimally intrusive separating inputs (i.e., inputs that deviate slightly from normal operation and create unique outputs belonging to at most one fault, for all uncertainties) for linear discrete-time systems. They illustrated the method guarantees of fault diagnosis using numerical examples, highlighting the ability to reach conclusions in finite time and the improved computational efficiency. Streif et al. (2013) studied the implications of uncertain inputs and created a method for certifying the robustness of active FDI by calculating uncertain input signals that separate outputs (of different fault scenarios) in a finite number of steps. They did so while minimizing the number of outputs and measurement samples required for robustness in order to subsequently reduce costs. Palmer et al. (2016) developed a methodology for optimally designing IBIT using techniques from the field of optimal experimental design and a frequentist inference approach for uncertainty. However, a drawback of all these methods is that they require knowledge on the probabilistic information of the uncertain inputs and parameters *a priori*. This statistical information is not always available, especially for fault scenarios that occur infrequently. In this case, other FDI methods are required to guarantee system safety.

When uncertainty cannot be quantified probabilistically or when robustness certificates are required for an FDI test at the bounds of uncertainty, a deterministic global method must be employed for the design of FDI tests. A useful technique for this case is known as worst-case optimization, of which the only requirement is that the design variables be bounded finite sets. The worst-case approach is a specific subset of semi-infinite programming (SIP) that focuses on the optimization under uncertainty (Asprey and Macchietto, 2002; Stuber and Barton, 2015). This approach can be leveraged for robust FDI, specifically in determining the feasibility of detecting and isolating faults for safety-critical systems at the worst-case realization of uncertainty. However, the global solution of SIPs is far from trivial and has garnered interest from a vast range of communities (Floudas and Gounaris, 2009). These programs optimize an objective function dependent on a finite set of design variables, subject to an infinite number of inequality and equality constraints also dependent upon these design variables. The worst-case SIP approach has been explored in many applications such as optimal experimental design, (Asprey and Macchietto, 2002; Puschke et al., 2018; Walz et al., 2018), process design (Stuber et al., 2014), and parameter estimation (Bollas et al., 2009; Mitsos et al., 2009); however, finding solutions to these complex problems is still an open challenge. Kwak and Haug (1976) first addressed optimization with uncertainty by solving a bilevel program using first-order functional approximations. Halemane and Grossmann (1983) extended this work and explored a special case of SIPs called max-min/min-max by forming explicit functions from the equality constraints. Swaney and Grossmann (1985) developed two algorithms capable of solving these types of problems given specific convexity requirements. Stuber and Barton (2011) explored this further in terms of robustness for engineering applications with nonconvexities. They presented a deterministic global optimization algorithm based on the work of Bhattacharjee et al. (2005) that is dependent on solving the equality constraints approximately for an implicit function with a successive-substitution fixed-point iteration technique. Floudas et al. (2001) explored the issues of differentiability that exist for SIPs and present a rigorous deterministic algorithm that is capable of solving SIPs with twice-differentiable inequality and equality constraints. Mitsos et al. (2007) developed an algorithm capable of handling nonconvexities but was restricted to inequality constrained bilevel programs. Stuber and Barton (2015) further addressed this issue, developing an algorithm capable of solving general SIPs that do not rely on approximations of the objective function, inequality constraints, or equality constraints. The only requirements are that the objective function and inequality constraints are continuous, the equality constraints are once-differentiable, there exists a Slater point close to a minimizer, and a unique implicit function exists for the equality constraint.

In this work, we design a system health maintenance test (i.e., IBIT, referred simply as BIT herein) for active FDI through the

formulation of a worst-case SIP. The goal of this test is to reduce, if not eliminate, false alarms, no fault founds, and nondetections common in uncertain systems. This is accomplished by solving the worst-case SIP globally for a feasible FDI test that is robust to all realizations of uncertainty. In Section 2, we present the mathematical formulation of our model-based active FDI method in the form of a worst-case implicit SIP. We then discuss the algorithms used to solve this problem and go into additional detail about the *a posteriori* classification used to compare different BIT designs. Section 3 then presents the application of this formulation to a benchmark three-tank system with several faults and uncertainties. We conclude this work by discussing the challenges of solving worst-case SIPs globally for (even) simple systems such as the one used in this work and show the value of the global BIT feasible solution.

The novelty of this work lies in the deterministic method for providing rigorous global guarantees of robustness in FDI which is particularly beneficial to safety-critical systems where instances of uncertainty may hide the root cause of faults that lead to catastrophic failures. The presented algorithm globally solves a semi-infinite program for the worst-case design of FDI tests that satisfy safety constraints over the entire uncertainty domain. Contributions of this work include the mathematical formulation of a semi-infinite program with implicit functions embedded, its application to a benchmark three-tank system with local and global solutions of maximum FDI effectiveness at the worst-case realization of uncertainty, and the comparison of test designs deployment using k-NN classification.

2. Methods

2.1. Model definition

The system of steady state algebraic equations describing the system of interest for robust FDI is defined as:

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

where $\mathbf{f}^{[f]} : D_{\tilde{x}^{[f]}} \times D_u \times D_{\theta_u} \times D_{\theta_f^{[f]}} \to \mathbb{R}^{N_{\tilde{x}}}$ is the system of equations that are assumed to be continuously differentiable and factorable (i.e., made up of elementary and transcendental functions) over its open domain $D_{\tilde{x}^{[f]}} \subset \mathbb{R}^{N_{\tilde{x}}}$, $D_u \subset \mathbb{R}^{N_u}$, $D_{\theta_u} \subset \mathbb{R}^{N_{\theta_u}}$, $D_{\theta_f^{[f]}} \subset \mathbb{R}^{N_{\theta_f}}$. The superscript $[f]$ denotes the fault scenario of interest and N_f is the total number of faults studied (with $[f] = [0]$ representing the fault-free system). The variable $\tilde{\mathbf{x}}^{[f]} \in D_{\tilde{x}^{[f]}} \subset \mathbb{R}^{N_{\tilde{x}}}$ is the vector of system states, $\mathbf{u} \in U = \{\mathbf{u} \in \mathbb{R}^{N_u} : \mathbf{u}^L \le \mathbf{u} \le \mathbf{u}^U\}$ is the vector of admissible system inputs, $\theta_u \in \Theta_u = \{\theta_u \in \mathbb{R}^{N_{\theta_u}} : \theta_u^L \le \theta_u \le \theta_u^U\}$ is the vector of uncertain parameters, and $\theta_f^{[f]} \in \Theta_f^{[f]} = \{\theta_f^{[f]} \in \mathbb{R}^{N_{\theta_f}} : \theta_f^{[f]^L} \le \theta_f^{[f]} \le \theta_f^{[f]^U}\}$ is the vector of parameters corresponding to faults. The system outputs are expressed as:

$$\mathbf{y}^{[f]} = \mathbf{h}(\tilde{\mathbf{x}}^{[f]}) + \mathbf{w}, \quad \forall [f] \in \{[0], \ldots, [N_f]\} \tag{2}$$

where $\mathbf{y}^{[f]} \in Y \subset \mathbb{R}^{N_y}$ is the vector of system outputs corresponding to $[f]$, $\mathbf{h}$ is the system of equations mapping the system states to the measured outputs, and $\mathbf{w} \in W \subset \mathbb{R}^{N_y}$ is the vector of measurement noise.

2.2. Implicit SIP formulation of worst-case BIT design

The objective of model-based active FDI methods implemented during system fault diagnostics (i.e., BIT) is to utilize the system model (1) and its outputs (2) to detect and isolate faults through a direct comparison with the measured outputs of the system. However, as discussed earlier, challenges arise when fault scenarios are not unique in their model outputs or are masked by uncertainty (e.g., measurement noise, input disturbances, fault severity, model inaccuracy) or control loops (Khan et al., 2014a; 2014b; Mesbah et al., 2014). It is, therefore, important to study the performance of fault diagnostics in systems subject to uncertainty, particularly at the worst-case realization for safety-critical systems. A worst-case "robust" BIT design shall fully detect and isolate all the potential faults over the entirety of the aforementioned uncertainty domain. This problem can be described mathematically as a min-max problem of the following form:

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

where $G : D_{\tilde{x}} \times D_u \times \times D_{\theta_u} \times D_{\theta_f} \to \mathbb{R}$ is the continuous and factorable feasibility criterion that defines the quality of the BIT design and $\mathbf{f}(\tilde{\mathbf{x}}, \mathbf{u}, \theta_u, \theta_f) = (\mathbf{f}^{[0]}, \ldots, \mathbf{f}^{[N_f]}) = 0$ is the combined system of steady state algebraic equations for all fault scenarios from (1) with augmented state variables $\tilde{\mathbf{x}} = (\tilde{\mathbf{x}}^{[0]}, \ldots, \tilde{\mathbf{x}}^{[N_f]}) \in \tilde{X} \subset \mathbb{R}^{N_{\tilde{x}}(N_f+1)}$ and parameters corresponding to faults $\theta_f = (\theta_f^{[0]}, \ldots, \theta_f^{[N_f]}) \in \Theta_f \subset \mathbb{R}^{N_{\theta_f}(N_f+1)}$.

The general nonconvex equality-constrained min-max problem presented in (3) is computationally intractable and not addressable by existing algorithms which are guaranteed finite termination (Stuber and Barton, 2015). With some mild assumptions from implicit function theory, if at least one $\tilde{\mathbf{x}}$ exists that satisfies (1) for each $(\mathbf{u}, \theta_u, \theta_f) \in U \times \Theta_u \times \Theta_f \subset D_u \times D_{\theta_u} \times D_{\theta_f}$, then it defines an implicit function $\mathbf{x} : U \times \times \Theta_u \times \Theta_f \to X$ of $(\mathbf{u}, \theta_u, \theta_f)$, expressed as $\tilde{\mathbf{x}} = \mathbf{x}(\mathbf{u}, \theta_u, \theta_f)$. Given the existence and uniqueness of the implicit function, such that $\mathbf{f}(\mathbf{x}(\mathbf{u}, \theta_u, \theta_f), \mathbf{u}, \theta_u, \theta_f) = 0$, $\forall (\mathbf{u}, \theta_u, \theta_f) \in U \times \Theta_u \times \Theta_f$ with $X \subset D_{\tilde{x}}$, the equality constraints of (3) can be eliminated to formulate an equivalent and more computationally tractable implicit min-max problem:

$$G^* = \min_{\mathbf{u}\in U} \max_{\theta_u\in\Theta_u,\, \theta_f\in\Theta_f} G(\mathbf{x}(\mathbf{u}, \theta_u, \theta_f), \mathbf{u}, \theta_u, \theta_f) \tag{4}$$

which can then be reformulated using standard optimization convention as an implicit SIP below:

$$\begin{aligned} \eta^* = \min_{\mathbf{u}\in U,\ \eta\in H} & \ \eta \\ \text{s.t. } \eta \ge & \max_{\theta_u\in\Theta_u,\, \theta_f\in\Theta_f} G(\mathbf{x}(\mathbf{u}, \theta_u, \theta_f), \mathbf{u}, \theta_u, \theta_f) \end{aligned} \tag{5}$$

where $\eta \in H \subset \mathbb{R}$ is an auxiliary variable introduced for the SIP formulation. The inner minimization program of (5) can be expressed in the following way by using the standard optimization convention of inequality constraints as nonpositive:

$$\begin{aligned} 0 \ge & \max_{\theta_u\in\Theta_u,\, \theta_f\in\Theta_f} G(\mathbf{x}(\mathbf{u}, \theta_u, \theta_f), \mathbf{u}, \theta_u, \theta_f) - \eta \iff \\ & G(\mathbf{x}(\mathbf{u}, \theta_u, \theta_f), \mathbf{u}, \theta_u, \theta_f) - \eta \le 0, \quad \forall\ (\theta_u, \theta_f) \in \Theta_u \times \Theta_f, \end{aligned} \tag{6}$$

which is referred to as the (implicit) semi-infinite constraint. Furthermore, through algebraic manipulation of the inequality constraint of (5) with (6) and the following identity, $g(\mathbf{x}(\mathbf{u}, \theta_u, \theta_f), \mathbf{u}, \theta_u, \theta_f, \eta) = G(\mathbf{x}(\mathbf{u}, \theta_u, \theta_f), \mathbf{u}, \theta_u, \theta_f) - \eta$, the previous implicit SIP (5) can be formulated as:

$$\begin{aligned} \eta^* = \min_{\mathbf{u}\in U,\ \eta\in H} & \ \eta \\ \text{s.t. } & g(\mathbf{x}(\mathbf{u}, \theta_u, \theta_f), \mathbf{u}, \theta_u, \theta_f, \eta) \le 0, \quad \forall\ (\theta_u, \theta_f) \in \Theta_u \times \Theta_f \end{aligned} \tag{7}$$

where g is the continuous and factorable semi-infinite constraint. This finalized formulation is in the "standard form" required by the implicit SIP algorithm used in this work. A feasible optimal solution to (7) coincides with $g \le 0$ for all realizations of uncertainty.

Furthermore, an optimal solution $\eta^* \leq 0$ implies $G^* \leq 0$, and conversely $\eta^* > 0$ implies $G^* > 0$.

2.3. Local and global solutions of implicit SIPs

The program (7) has a finite number of variables yet an infinite number of constraints, due to g being indexed by the compact parameter sets of the uncertainty and fault domains. The infinite number of constraints introduces significant complexity over standard nonlinear programs (NLPs) and as such, SIPs are extremely difficult to solve, and often intractable. Hettich and Kortanek (1993) highlighted that these problems are typically constructed into finite equivalents and solved using conventional algorithms. A similar type of problem was solved by Asprey and Macchietto (2002) using Algorithm 1. This algorithm is the general alternating procedure presented by Blankenship and Falk (1976) that consists of utilizing cutting planes to approximate the solution of (7). By solving a sequence of auxiliary optimization problems, nonlinear cuts are generated (i.e., new constraints are added) based on the most violating constraint at the current approximate solution until the algorithm converges to a solution to (7). This algorithm requires an assumption on convexity, as the objective function of Asprey and Macchietto (2002) is convex in nature (DeCock et al., 2016), and this assumption is tested in this work to explore the algorithm's finite convergence. Algorithm 1 holds for systems with bounded uncertainties, which is often the case for engineered systems and the system studied here.

Algorithm 1 SIP Min-Max Algorithm.

Require: $\theta_u^{(1)} \in \Theta_u, \theta_f^{(1)} \in \Theta_f, K \leftarrow 1$

1: **while** $\hat{\eta}^{(K)} < \eta^{(K)} \wedge K \leq K_{\max}$ **do**
2: Solve (7) while satisfying its semi-infinite constraint at $(\theta_u^{(k)}, \theta_f^{(k)}),\ \forall k \in \{1, \ldots, K\}$.
Store the optimal solution and objective as $(\eta^{(K)}, \mathbf{u}^{(K)})$.
3: $(\hat{\eta}^{(K)}, \theta_u^{(K+1)}, \theta_f^{(K+1)}) \leftarrow \max_{\theta_u \in \Theta_u, \theta_f \in \Theta_f} G(\mathbf{x}(\mathbf{u}^{(K)}, \theta_u, \theta_f), \mathbf{u}^{(K)}, \theta_u, \theta_f)$
4: $K \leftarrow K + 1$
5: **end**
6: **if** $K \leq K_{\max}$ **then**
7: $(\eta^*, \mathbf{u}^*, \theta_u^*, \theta_f^*) \leftarrow (\hat{\eta}^{(K-1)}, \mathbf{u}^{(K-1)}, \theta_u^{(K)}, \theta_f^{(K)})$
8: **Terminate**: Feasible Design
9: **else**
10: **Terminate**: Infeasible Design
11: **end**

Algorithm 1 solves (7) 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 of that iteration 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 Algorithm 1 seems to be sufficient for the application presented in Section 3, global methods are required to guarantee feasibility in cases when this assumption fails. Global methods avoid potentially suboptimal local solutions caused by nonconvexities in SIPs. Falk and Hoffman (1977) extend upon Blankenship and Falk (1976)'s cutting-plane algorithm for solving nonlinear explicit SIPs to examine large classes of nonconvex functions. Mitsos (2011) improved upon the Blankenship and Falk (1976) algorithm by utilizing an upper-bounding procedure that perturbs the right-hand side of the semi-infinite constraint in (7), guaranteeing the generation of SIP-feasible points in a finite manner for continuous NLPs that contain Slater points. Stuber and Barton (2015) adapted the work of Mitsos (2011) to allow for its application to implicit SIPs, and is the method used here for the worst-case-scenario design of FDI tests in systems under uncertainty. In general, the algorithm depends on the capability of solving three nonconvex NLPs to global optimality at each iteration. The extension of this algorithm to implicit SIPs follows the same Slater point requirement and was guaranteed to finitely converge to a global optimal by Stuber et al. (2015) for each implicit NLP subproblem. These three subproblems are referred herein as the lower-bounding program, the inner program, and the upper-bounding program, and their application to implicit SIPs is summarized in Algorithm 2 and explained below.

2.3.1. Lower-bounding program

The lower-bounding program discussed above is the first of the three subproblems solved in the global implicit SIP algorithm of Stuber et al. (2014). This program is a relaxation of the original implicit SIP to an implicit NLP with a finite number of constraints. These constraints correspond to the finite number of uncertainty realizations $(\theta_u, \theta_f) \in \Theta_u^{LBP} \times \Theta_f^{LBP} \subset \Theta_u \times \Theta_f$ in the reduced set of the lower-bounding program. The lower-bounding program is formulated as:

$$\begin{aligned} \eta^{LBP} = \min_{\mathbf{u} \in U,\ \eta \in H}\ & \eta \\ \text{s.t. } & g(\mathbf{x}(\mathbf{u}, \theta_u, \theta_f), \mathbf{u}, \theta_u, \theta_f, \eta) \leq 0, \\ & \forall\ (\theta_u, \theta_f) \in \Theta_u^{LBP} \times \Theta_f^{LBP} \subset \Theta_u \times \Theta_f \end{aligned} \tag{8}$$

A global solution of (8) guarantees that η^{LBP} is a rigorous bound.

2.3.2. Inner program

The second program of Algorithm 2 is the inner program. The inner program is equivalent to the semi-infinite constraint of the original SIP (7) and defines the SIP feasible region given a candidate point $(\bar{\mathbf{u}}, \bar{\eta}) \in U \times H$, formulated as:

$$\tilde{g}(\bar{\mathbf{u}}, \bar{\eta}) = \max_{\theta_f \in \Theta_f,\ \theta_u \in \Theta_u} g(\mathbf{x}(\bar{\mathbf{u}}, \theta_u, \theta_f), \bar{\mathbf{u}}, \theta_u, \theta_f, \bar{\eta}) \tag{9}$$

The candidate point $(\bar{\mathbf{u}}, \bar{\eta})$ is determined to be a feasible point of (7) if $\tilde{g}(\bar{\mathbf{u}}, \bar{\eta}) \leq 0$, provided that the nonconvex NLP (9) is solved to global optimality.

2.3.3. Upper-bounding program

The third and final program of Algorithm 2 is the novel upper-bounding program (Mitsos, 2011). Similar to the lower-bounding program, the original SIP is reduced to an implicit NLP with a finite number of constraints corresponding to realizations of uncertainty in its own reduced set $(\theta_u, \theta_f) \in \Theta_u^{UBP} \times \Theta_f^{UBP} \subset \Theta_u \times \Theta_f$. However, the upper-bounding program also contains a restricting parameter $\epsilon^g > 0$ that perturbs the right-hand side of the semi-infinite constraint away from zero, formulated as:

$$\begin{aligned} \eta^{UBP} = \min_{\mathbf{u} \in U,\ \eta \in H}\ & \eta \\ \text{s.t. } & g(\mathbf{x}(\mathbf{u}, \theta_u, \theta_f), \mathbf{u}, \theta_u, \theta_f, \eta) \leq -\epsilon^g, \\ & \forall\ (\theta_u, \theta_f) \in \Theta_u^{UBP} \times \Theta_f^{UBP} \subset \Theta_u \times \Theta_f \end{aligned} \tag{10}$$

If there exists an SIP-Slater point, the algorithm is guaranteed to generate a sequence of feasible points and converge to an ϵ^g-optimal feasible solution in finitely-many iterations.

Algorithm 2 Implicit SIP Global Optimization Algorithm.

Require: $LB = -\infty$, $UB = +\infty$, $\epsilon_{tol} > 0$, $K \leftarrow 0$, $\theta_u^{LBP} = \theta_u^{LBP,0}$, $\theta_u^{UBP} = \theta_u^{UBP,0}$, $\theta_f^{LBP} = \theta_f^{LBP,0}$, $\theta_f^{UBP} = \theta_f^{UBP,0}$,$\epsilon^g \leftarrow \epsilon^{g,0} > 0$, and $r > 1$

while $UB - LB \geq \epsilon_{tol}$ **do**
  solve LBP (8) for optimal solution $\mathbf{u}^{LBP}$ and objective value η^{LBP}
  $LB \leftarrow \eta^{LBP}$, $\tilde{\mathbf{u}} \leftarrow \mathbf{u}^{LBP}$, $\tilde{\eta} \leftarrow \eta^{LBP}$
  if $LB > 0$ **then**
    Terminate: Infeasible Design
  else
    Solve IP (9) for optimal objective value $\tilde{g}(\tilde{\mathbf{u}}, \tilde{\eta})$ and uncertainty θ_u^{IP}, θ_f^{IP}
  end
  if $\tilde{g}(\tilde{\mathbf{u}}, \tilde{\eta}) \leq 0$ **then**
    $\mathbf{u}^* \leftarrow \tilde{\mathbf{u}}$, $\eta^* \leftarrow \tilde{\eta}$
    if $\eta^* \leq 0$ **then**
      Terminate: Feasible Design
    else
      Terminate: Infeasible Design
    end
  else
    $\theta_u^{IP} \rightarrow \Theta_u^{LBP}$, $\theta_f^{IP} \rightarrow \Theta_f^{LBP}$
  end
  solve UBP (10) for optimal solution $\mathbf{u}^{UBP}$ and objective value η^{UBP}
  if UBP (10) is feasible **then**
    $\tilde{\mathbf{u}} \leftarrow \mathbf{u}^{UBP}$, $\tilde{\eta} \leftarrow \eta^{UBP}$
    Solve IP (9) for optimal objective value $\tilde{g}(\tilde{\mathbf{u}}, \tilde{\eta})$ and uncertainty θ_u^{IP}, θ_f^{IP}
    if $\tilde{g}(\tilde{\mathbf{u}}, \tilde{\eta}) < 0$ **then**
      if $\eta^{UBP} \leq 0$ **then**
        Terminate: Feasible Design
      else
        if $\tilde{\eta} < UB$ **then**
          $\mathbf{u}^* \leftarrow \tilde{\mathbf{u}}$, $UB \leftarrow \tilde{\eta}$
        end
        $\epsilon^{g,K+1} \leftarrow \epsilon^{g,K}/r$
      end
    else
      $\theta_u^{IP} \rightarrow \Theta_u^{UBP}$, $\theta_f^{IP} \rightarrow \Theta_f^{UBP}$
    end
  else
    $\epsilon^{g,K+1} \leftarrow \epsilon^{g,K}/r$
  end
  $K \leftarrow K + 1$
end
Terminate: Unknown

2.3.4. Implicit SIP global algorithm

The three subproblems above are all used in the implicit global SIP algorithm, Algorithm 2. The solutions to subproblems (8) and (10) maintain the following relationship,

$$LB = \eta^{LBP} \leq \eta^* \leq \eta^{UBP} = UB.$$

The algorithm solves the original SIP (7) to ϵ_{tol} optimality in a finite number of iterations given the mild assumptions laid out by Stuber and Barton (2015). Algorithm 2 overviews the procedure used for solving the implicit SIP of this work with the early termination criteria used in Stuber et al. (2014). The addition of these criteria significantly improves the algorithm efficiency by preventing the unnecessary effort of solving (7) to global optimality in cases where guarantees of feasibility or infeasibility can be made prior. It is noteworthy to clarify that "**Terminate**: Unknown" indicates the rare case when $\eta^* = 0$ and the algorithm converges with $\epsilon_{tol} - optimality$ after finitely many iterations. In this case, no rigorous guarantees of design feasibility can be made and further investigation is required.

2.4. k-NN classification for FDI deployment

After design of the FDI test, a robust and computationally efficient method is deployed for the classification of the faults under consideration. As discussed in the introduction, there exist ample passive FDI techniques to choose from such as neural networks, principal component analysis, and support vector machines (Gajjar et al., 2018; Moosavian et al., 2013; Najjar et al., 2016; Onel et al., 2018a; 2018b; Shahnazari et al., 2018; Tamura and Tsujita, 2007; Yu, 2013). The k-nearest neighbors (k-NN) algorithm was chosen for this work because of its simple procedure and the dimensionality of the data being processed is minimal. For data sets that are large in dimension, additional measures (e.g., PCA) need to be taken to reduce the number of features analyzed in k-NN, such as the work done by Gajjar et al. (2018) and Onel et al. (2018a,b) on fault detection and diagnosis for Big Data.

The k-NN method of classification can be described as a method of supervised learning that attempts to classify a given observation $\mathbf{y} = (y_1, \ldots, y_{N_y})$ to the class $c^{[f]}$ with the highest estimated probability, where $\mathbf{y}$ is a sampled system observation of unknown class $c^{\mathbf{y}}$ (i.e., fault scenario) used for FDI. This is accomplished by first obtaining a training data set of historical observations $Y^{\text{train}} \subset \mathbb{R}^{N_{\text{train}}(N_f+1)\times N_y}$ and their respective classes $C^{\text{train}} = \{c_1^{\text{train}}, \ldots, c_{N_{\text{train}}(N_f+1)}^{\text{train}}\}$. The training data set used in this work is obtained from running N_{train} Monte Carlo simulations over the uncertainty domain. Afterwards, a positive integer k (usually odd to avoid ties in classification decisions) and $\mathbf{y}$ is provided. The k-NN classifier then finds the k training data points $Y^{k\text{-NN}} \subset \mathbb{R}^{k\times N_y}$ of class $C^{k\text{-NN}} = \{c_1^{k\text{-NN}}, \ldots, c_k^{k\text{-NN}}\}$ closest to $\mathbf{y}$. A standard metric used to determine how close points are to the observation is the Euclidean distance; however, other metrics such as the Manhattan, Chebyshev, and Hamming distances can be used in special circumstances for k-NN. Next, the conditional probability of each class $c^{[f]}$, $[f] = [0], \ldots, [N_f]$, for each individual observation y_i, $i = 1, \ldots, N_y$, is estimated as the fraction of points in $Y^{k\text{-NN}}$ with $c^{k\text{-NN}} = c^{[f]}$:

$$P_i(c^{\mathbf{y}} = c^{[f]}|y_i) = \frac{1}{k}\sum_{j=1}^{k}\begin{cases}1, & \text{if } c_j^{k\text{-NN}} = c^{[f]}\\ 0, & \text{otherwise}\end{cases},$$
$$\forall([f], i) \in \{[0], \ldots, [N_f]\} \times \{1, \ldots, N_y\}, \quad (11)$$

Lastly, the class that $\mathbf{y}$ belongs to is estimated using a majority vote of the individual observation's conditional probabilities P_i, $i = 1, \ldots, N_y$, each weighted with their respective predetermined factor α_i, $i = 1, \ldots, N_y$. The concluding class is the one with the highest majority vote based on conditional probability, defined as:

$$\hat{c}^{[j]} : j \in \arg\max_{[f]\in\{[0],\ldots,[N_f]\}} P\left(c^{\mathbf{y}} = c^{[f]}|\mathbf{y}\right) = \sum_{i=1}^{N_y}\alpha_i P_i\left(c^{\mathbf{y}} = c^{[f]}|y_i\right), \quad (12)$$

In this work we use equal voting (i.e., $\alpha_i = N_y^{-1}$, $i = 1, \ldots, N_y$) but this may not always be ideal in situations where some observations are more reliable than others.

The overall accuracy of the k-NN classification is then gauged by running N_{test} Monte Carlo simulations to create a new set of observations $Y^{\text{test}} \subset \mathbb{R}^{N_{\text{test}}(N_f+1)\times N_y}$ of class $C^{\text{test}} = \{c_1^{\text{test}}, \ldots, c_{N_{\text{test}}(N_f+1)}^{\text{test}}\}$, independent from the training data Y^{train}.

Each test observation is classified using the trained k-NN according to (12), and the percentage of correct classifications is calculated as:

$$A_{cc} = \frac{1}{N_{\text{test}}(N_f+1)} \sum_{n=1}^{N_{\text{test}}(N_f+1)} \begin{cases} 1, & \text{if } \hat{c}_n^{[j]} = c_n^{\text{test}} \\ 0, & \text{otherwise} \end{cases} \tag{13}$$

where $\hat{c}_n^{[j]}$ is the estimated class of test observation $\mathbf{y}_n$ from (12) and c_n^{test} is the actual class of $\mathbf{y}_n$.

3. Results and discussion

As discussed earlier, the instantiation of uncertainty, particularly at its worst-case scenario, during system operation and maintenance plays a major role in negatively impacting system health and safety. A timely example (at the time of writing) of this challenge is discussed by NASA (Belcastro, 2011), in their study on aircraft loss of control (LOC) scenarios. Belcastro (2011) assessed that 45.2% of LOC accidents in aircraft is due to system faults, which translates to 46.1% of fatalities due to these accidents. Effective detection under off-nominal conditions is cited as a future solution to mitigate these issues. Specifically, in-situ estimation methods for distinguishing between anomalous system behavior and external disturbances are discussed as critical in future health management systems for aircraft. The role of robustness to uncertainty, mitigation of false alarms and misclassifications, is highlighted as a critical need for the aerospace industry, wherein systems are often safety-critical. For these type of systems, the methodology of Section 2 can provide rigorous global guarantees on system safety, which is critical for the certification of these systems. In this section we illustrate the application and benefits of the method in a relevant open-literature case study of the benchmark three-tank system. The "safety-critical" fault in this scenario is a tank leak and pump degradation, with the system affected by many sources of uncertainty which can lead to overflow and system shut-down.

3.1. Three-tank system model equations

The methods described are applied for FDI in a benchmark three-tank system, studied in Mesbah et al. (2014), to illustrate robustness. This system has $N_{\tilde{x}} = 3$, $N_u = 2$, $N_{\theta_u} = 3$, $N_{\theta_f} = 2$, $N_y = 3$, and $N_f = 3$. The layout of the three-tank system and its respective inputs $\mathbf{u}$, states $\tilde{\mathbf{x}}$, uncertain parameters θ_u, and parameters representing fault θ_f are shown in Fig. 1. The cylindrical tanks, Tank 1, Tank 2, and Tank 3, have equal cross-sectional area $A_T = 0.0154\ m^2$ and height $\tilde{x}^{\max} = 0.75\ m$. The two admissible system inputs are the assigned flow rates of Pump 1 and Pump 2: u_1 and u_2 $(m^3 s^{-1})$. The tank connecting pipes and exiting pipe have equal cross-sectional area $A_p = 0.00005\ \text{m}^2$. The flow of liquid through these pipes is characterized by the nondimensional flow coefficients k_{c_1}, k_{c_2}, and k_{c_3}. The system state $\tilde{x}_i^{[f]}$ (m) corresponds to the liquid height of Tank i for the given fault scenario $[f]$. The system is studied at the fault-free case ($[f] = [0]$) with uncertainties present. Additionally, three uncertain fault scenarios are studied: Pump 1 degradation ($[f] = [1]$), Tank 2 leak ($[f] = [2]$), and simultaneous Pump 1 degradation and Tank 2 leak ($[f] = [3]$). The Pump 1 degradation fault scenario is characterized by the nondimensional coefficient $\beta^{[f]}$ ($\beta^{[0],[2]} = 1$). The flow rate supplied to Tank 1 is proportional to u_1 and $\beta^{[f]}$. The Tank 2 leak fault scenario is characterized by the circular hole radius $r^{[f]}$ ($r^{[0],[1]} = 0\ m$). It is assumed that this leak has the same flow characteristics as the liquid exiting Tank 2.

To recap, the liquid heights of Tank 1, Tank 2, and Tank 3 are the system states $\tilde{\mathbf{x}}^{[f]} = (\tilde{x}_1^{[f]}, \tilde{x}_2^{[f]}, \tilde{x}_3^{[f]})$, $[f] = [0], \ldots, [3]$. The assigned liquid flow rates of Pump 1 and Pump 2 are the admissible system inputs $\mathbf{u} = (u_1, u_2)$. The flow coefficients are the uncertain parameters $\theta_u = (k_{c_1}, k_{c_2}, k_{c_3})$. The pump degradation coefficient and leak radius are the parameters representing faults $\theta_f^{[f]} = (\beta^{[f]}, r^{[f]})$. In addition, the outputs are assumed to be void of noise ($\mathbf{w} = \mathbf{0}$), augmented for each fault scenario as such $\mathbf{y}^{[f]} = (y_1^{[f]}, y_2^{[f]}, y_3^{[f]}) = \tilde{\mathbf{x}}^{[f]}$, $[f] = [0], \ldots, [3]$.

The dynamic model of the three-tank system studied was derived from Torricelli's law, and is the system of equations shown below for each fault scenario:

$$\begin{aligned} A_T \dot{\tilde{\mathbf{x}}}^{[f]} &= \mathbf{f}^{[f]}(\tilde{\mathbf{x}}^{[f]}, \mathbf{u}, \theta_u, \theta_f^{[f]}) \\ &= \begin{pmatrix} -k_{c_1} A_P sgn(\tilde{x}_1^{[f]} - \tilde{x}_3^{[f]}) \sqrt{2\ g \left| \tilde{x}_1^{[f]} - \tilde{x}_3^{[f]} \right|} + u_1 + (\beta^{[f]} - 1) u_1 \\ -k_{c_3} A_P sgn(\tilde{x}_2^{[f]} - \tilde{x}_3^{[f]}) \sqrt{2\ g \left| \tilde{x}_2^{[f]} - \tilde{x}_3^{[f]} \right|} - k_{c_2} A_P \sqrt{2\ g \tilde{x}_2^{[f]}} - k_{c_2} \pi r^{[f]2} \sqrt{2\ g \tilde{x}_2^{[f]}} + u_2 \\ k_{c_1} A_P sgn(\tilde{x}_1^{[f]} - \tilde{x}_3^{[f]}) \sqrt{2\ g \left| \tilde{x}_1^{[f]} - \tilde{x}_3^{[f]} \right|} - k_{c_3} A_P sgn(\tilde{x}_3^{[f]} - \tilde{x}_2^{[f]}) \sqrt{2\ g \left| \tilde{x}_3^{[f]} - \tilde{x}_2^{[f]} \right|} \end{pmatrix}, \\ &\forall [f] \in \{[0], [1], [2], [3]\} \end{aligned} \tag{14}$$

where $\dot{\tilde{\mathbf{x}}}^{[f]} \in D_{\dot{\tilde{x}}[f]} \subset \mathbb{R}^{N_{\tilde{x}}}$ is the vector of state variable time derivatives. To obtain the steady state equations used in this work, the left-hand side derivative term $A_T \dot{\tilde{\mathbf{x}}}^{[f]}$ was set to zero. In order to use the solvers and algorithms that provide global guarantees, approximations of (14) must be introduced to ensure continuity and differentiability (i.e., the signum and absolute value functions must be replaced by continuously differentiable approximations). The updated equations with sufficiently accurate approximations are presented in (15) in their steady state form:

$$\begin{aligned} &\mathbf{f}^{[f]}(\tilde{\mathbf{x}}^{[f]}, \mathbf{u}, \theta_u, \theta_f^{[f]}) = \mathbf{0} \\ &= \begin{pmatrix} -k_{c_1} A_P \tanh(\delta \Delta \tilde{x}_{13}^{[f]}) \sqrt{2\ g \sqrt{(\Delta \tilde{x}_{13}^{[f]})^2 + \epsilon^2}} \\ \qquad + u_1 + (\beta^{[f]} - 1) u_1 \\ -k_{c_3} A_P \tanh(\delta \Delta \tilde{x}_{23}^{[f]}) \sqrt{2\ g \sqrt{(\Delta \tilde{x}_{23}^{[f]})^2 + \epsilon^2}} \\ \qquad - k_{c_2} A_P \sqrt{2\ g \tilde{x}_2^{[f]}} - k_{c_2} \pi r^{[f]2} \sqrt{2\ g \tilde{x}_2^{[f]}} + u_2 \\ k_{c_1} A_P \tanh(\delta \Delta \tilde{x}_{13}^{[f]}) \sqrt{2\ g \sqrt{(\Delta \tilde{x}_{13}^{[f]})^2 + \epsilon^2}} \\ \qquad - k_{c_3} A_P \tanh(\delta \Delta \tilde{x}_{32}^{[f]}) \sqrt{2\ g \sqrt{(\Delta \tilde{x}_{32}^{[f]})^2 + \epsilon^2}} \end{pmatrix}, \\ &\forall [f] \in \{[0], [1], [2], [3]\} \end{aligned} \tag{15}$$

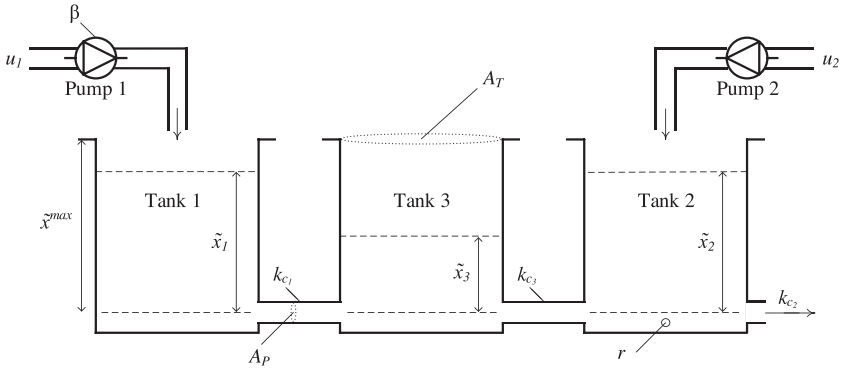


Fig. 1. Three-tank system model architecture from Mesbah et al. (2014) with labeled system states $\tilde{\mathbf{x}}^{[f]} = (\tilde{x}_1^{[f]}, \tilde{x}_2^{[f]}, \tilde{x}_3^{[f]})$, inputs $\mathbf{u} = (u_1, u_2)$, uncertain parameters $\theta_u = (k_{c_1}, k_{c_2}, k_{c_3})$, and fault parameters $\theta_f^{[f]} = (\beta^{[f]}, r^{[f]})$.

where $\Delta\tilde{x}_{ij}^{[f]} \equiv \tilde{x}_i^{[f]} - \tilde{x}_j^{[f]}$, $\tanh(\delta\Delta\tilde{x}_{ij}^{[f]})$ is a continuously differentiable approximation of the signum function, and $\sqrt{(\Delta\tilde{x}_{ij}^{[f]})^2 + \epsilon}$ is a continuously differentiable approximation of the absolute value function. These approximations were chosen based on their high accuracy and low order-of-magnitude derivatives when compared to their counterparts. It is important to note that to avoid numerical issues, a trade-off analysis between the error and stiffness of each approximation is required when determining the parametric values of δ and ϵ. For example, the error of the absolute value approximation is on the order of ϵ and converges to ϵ as $\Delta\tilde{x}_{ij}^{[f]} \to 0$. However, choosing small values of ϵ to minimize error can lead to large magnitude derivatives that diverge to $+\infty$ as $\epsilon \to 0$ which may introduce numerical issues for gradient-based optimizers.

3.2. SIP formulation of worst-case BIT design

It is crucial in fault diagnostics, particularly when designing BIT, to discern between a fault-free system with frequent disturbances and noise, and a system with fault(s). Thus, having a test that produces unique outputs in the presence of uncertainty for a fault-free system and all its potential faults is desirable. In this work, the objective function G used for designing BIT is the separation of outputs recorded for each fault scenario, defined as the sum of the squared differences below:

$$G(\mathbf{x}(\mathbf{u}, \theta_u, \theta_f), \mathbf{u}, \theta_u, \theta_f) = \eta^{feas} - \sum_{i=1}^{N_y} \sum_{f=0}^{N_f-1} \sum_{g=f+1}^{N_f} (y_i^{[f]} - y_i^{[g]})^2, \quad (16)$$

where $\eta^{feas} \in H^{feas} \subset \mathbb{R}$ is the feasibility parameter that specifies a desired FDI performance. The goal of the following method is to find an objective that is at least as great as this parameter (i.e., $G^* \geq \eta^{feas}$). Therefore, (16) is written using standard optimization convention so that a feasible solution found by Algorithm 2 results in $G^* \leq 0$. Updating the finalized implicit SIP formulation (7) with the objective (16) results in the finalized problem formulation solved in this work:

$$\begin{aligned} &\min_{\mathbf{u}\in U,\ \eta\in H} \ \eta \\ &\text{s.t. } \eta^{feas} - \left[\sum_{i=1}^{N_y} \sum_{f=0}^{N_f-1} \sum_{g=f+1}^{N_f} (y_i^{[f]} - y_i^{[g]})^2\right] \\ &\quad -\eta \leq 0 \ \forall \ (\theta_u, \theta_f) \in \Theta_u \times \Theta_f, \end{aligned} \quad (17)$$

An $\eta^* > 0$ implies that no feasible worst-case BIT design exists which is capable of producing the desired separation η^{feas} for all realizations of uncertainty in $\Theta_u \times \Theta_f$. On the contrary, $\eta^* \leq 0$ means that a feasible worst-case BIT design exists and the solution found is guaranteed to satisfy the BIT performance for all realizations of uncertainty.

The respective variable domains used in (17) are as follows: the augmented state interval is $\tilde{X} = [0, 0.75]^{12}$, bounded by the physical design constraint $\tilde{x}^{\max}$, the BIT design interval is $U = [10^{-5}, 10^{-4}]^2$, the uncertain 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 $H = [-0.1, 10]$, and the FDI performance parameter is $\eta_{feas} = 0.25$. It is assumed that an implicit function $\mathbf{x} : U \times \Theta_u \times \Theta_f \to X$ is enclosed upon these intervals, such that $\mathbf{f}(\mathbf{x}(\mathbf{u}, \theta_u, \theta_f), \mathbf{u}, \theta_u, \theta_f) = 0, \ \forall(\mathbf{u}, \theta_u, \theta_f) \in U \times \Theta_u \times \Theta_f$. The upper and lower bounds of the parameter domains were calculated as three sigma deviations from the mean $\mu \pm 3\sigma$, using the probabilistic information presented in Table 1. The only exception was the lower bound of the Tank 2 leak radius, whose three sigma deviation becomes negative which does not make physical sense. A hole size an order of magnitude smaller than the upper bound was decided upon as the lower bound.

3.3. Comparison of BIT designs for FDI

The three-tank system model Eqs. (15) were programmed using Julia (Bezanson et al., 2017). A simulation-based approach of obtaining an implicit function was implemented, and a robust worst-case BIT design solution to (17) was obtained using the JuMP interface and Algorithm 1. Additionally, this solution was verified globally for its SIP feasibility using the package EAGO (Wilhelm and Stuber, 0000) and Algorithm 2. For the sake of illustrating the benefit of the robust worst-case BIT design, labeled 'Worst-Case', three other BIT designs were analyzed and are presented in Table 2. The first BIT design, labeled as 'Nominal', consisted of equal inputs $\mathbf{u} = (4.1 \cdot 10^{-5}, 4.1 \cdot 10^{-5})$ near the midpoint of the original BIT design interval U. This design illustrates an example of a sub-optimal test that is heuristically chosen for maintenance. The worst-case realization of uncertainty at the 'Nominal' BIT design was solved from (17) with the restricted input domain $U = \left[4.1 \cdot 10^{-5}, 4.1 \cdot 10^{-5}\right]^2$. The second BIT design, labeled as 'Mean', represents a maintenance test intended for the anticipated faults and uncertainty. The mean μ parameter values of the faults and uncertainty can be found in Table 1. The 'Mean' BIT design was solved from (17) with the restricted uncertain and fault parameter domains $\Theta_u \times \Theta_f = [1.00, 1.00] \times [0.80, 0.80] \times [1.00, 1.00] \times [0.60, 0.60] \times [0.002, 0.002]$. The third BIT design, labeled as 'Conservative', represents a test that was developed iteratively after observing realizations of uncertainty at the 'Mean' design that led to constraint violations (this can be seen in Fig. 5(b)). An updated tank height constraint $\tilde{x}^{\max}$ was used in the 'Conservative' BIT

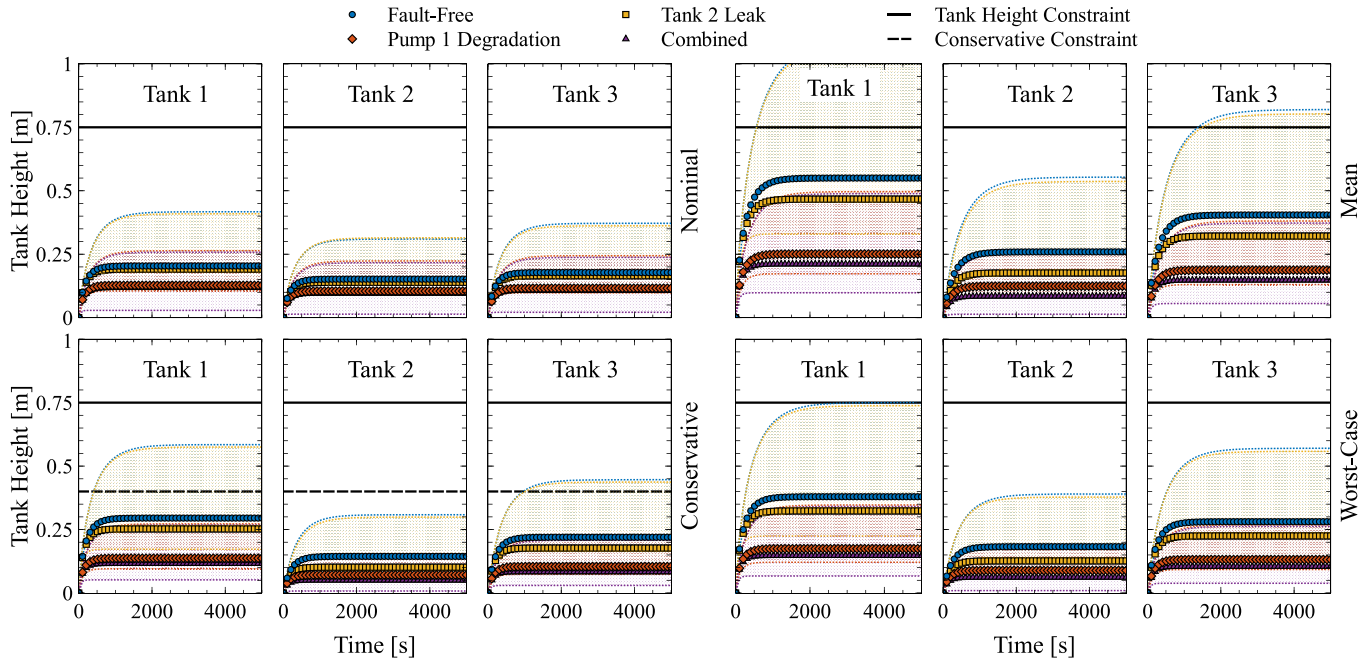


Fig. 2. Dynamic simulations of the three-tank system heights for the 4 BIT designs in Table 2 and the 4 fault scenarios at the worst-case realizations of uncertainty shown in Table 3. The black solid line represents the actual tank height constraint $\tilde{x}_{\max} = 0.75$. The black dashed line in the 'Conservative' design plot represents the updated tank height constraint $\tilde{x}_{\max} = 0.40$. The dotted shaded regions represent the ranges in tank heights for the different fault scenarios at other realizations of uncertainty.

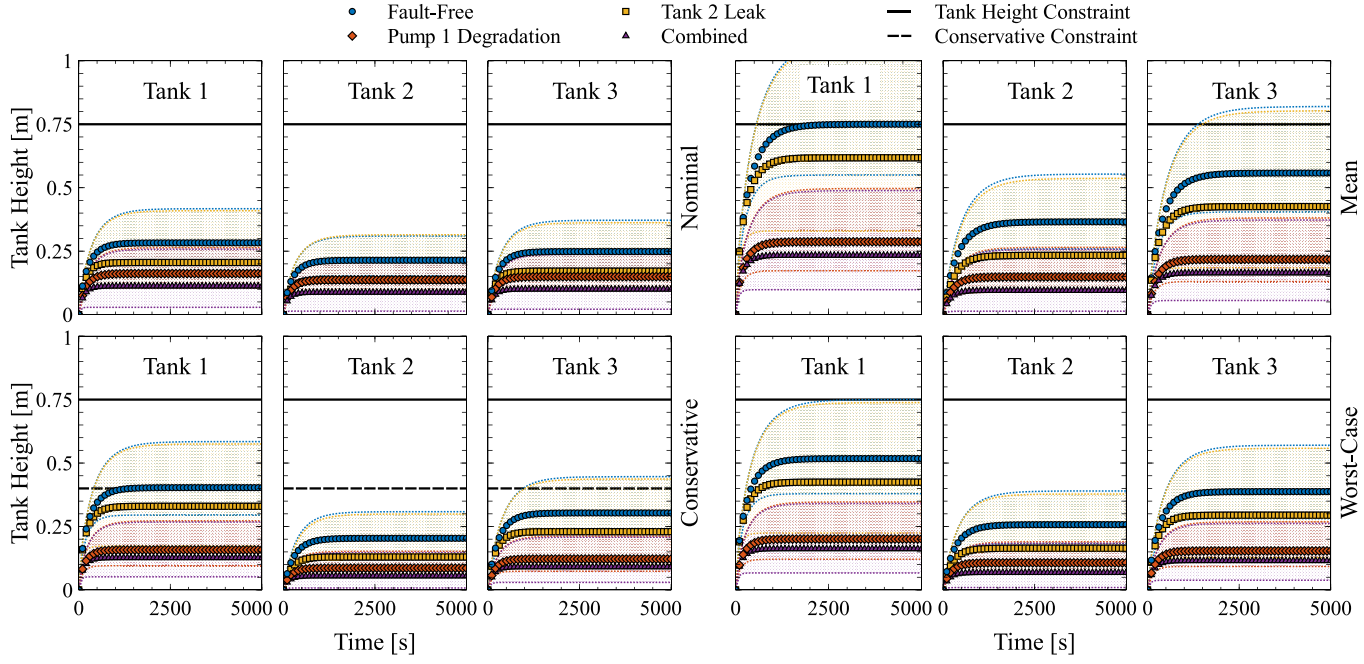


Fig. 3. Dynamic simulations of the three-tank system heights for the 4 BIT designs in Table 2 and the 4 fault scenarios at the anticipated realizations of uncertainty μ shown in Table 1. The black solid line represents the actual tank height constraint $\tilde{x}_{\max} = 0.75$. The black dashed line in the 'Conservative' design plot represents the updated tank height constraint $\tilde{x}_{\max} = 0.40$. The dotted shaded regions represent the ranges in tank heights for the different fault scenarios at other realizations of uncertainty.

design to reduce the risk of violation, based on the largest violation observed at the 'Mean' design. The new constraint was reduced from 0.75 to 0.40 for all three tanks due to a maximum violation of ≈ 0.35. The 'Conservative' BIT was solved from (17) with the same uncertain and fault parameter domains $\Theta_u \times \Theta_f$ used for the 'Mean' design and the updated state domain $\tilde{\mathbf{x}} \in \tilde{X} = [0, 0.40]^{12}$, given the new tank height constraint $\tilde{x}^{\max} = 0.40$ (shown in Figs. 2, 3, and 5(c)).

The worst-case realizations of uncertainty and faults (in terms of FDI performance) for the 4 BIT designs were obtained and displayed in Table 3. Using (14), the three-tank system was dynamically simulated for the 4 different BIT designs at their worst-case realizations of uncertainty and faults. The outputs of the 4 fault scenarios studied (i.e., fault-free, Pump 1 degradation, Tank 2 leak, and simultaneous) are shown in Fig. 2. Once steady state is achieved, these outputs are equivalent to the ones obtained from

Table 1
Description of the uncertainties $\theta_u = (k_{c_1}, k_{c_2}, k_{c_3})$ and faults $\theta_f^{[f]} = (\beta^{[f]}, r^{[f]})$ studied and their normally distributed $\mathcal{N}(\mu, \sigma^2)$ values with mean μ and variance σ^2 (Mesbah et al., 2014).

Faults and uncertainties	Parameters	Uncertainty distribution
Tank 1 Flow Coefficient	$\theta_{u,1} = k_{c_1}$	$\mathcal{N}(1.0, 2.5 \cdot 10^{-3})$
Tank 2 Flow Coefficient	$\theta_{u,2} = k_{c_2}$	$\mathcal{N}(0.8, 2.5 \cdot 10^{-3})$
Tank 3 Flow Coefficient	$\theta_{u,3} = k_{c_3}$	$\mathcal{N}(1.0, 2.5 \cdot 10^{-3})$
Pump 1 Degradation Coefficient	$\theta_{f,1}^{[f]} = \beta^{[f]}$	$\mathcal{N}(0.6, 4.0 \cdot 10^{-4})$
Tank 2 Leak Radius	$\theta_{f,2}^{[f]} = r^{[f]}$	$\mathcal{N}(2.0 \cdot 10^{-2}, 1.0 \cdot 10^{-6})$

Table 2
The input bounds and solutions to (17) for the different BIT designs.

Inputs $(m^3 s^{-1} \cdot 10^{-4})$	u_1^*	u_2^*	G^*
Minimum	0.10	0.10	–
Nominal	0.41	0.41	0.204
Mean	0.97	0.10	−0.314
Conservative	0.70	0.10	0.090
Worst-Case	0.80	0.10	−0.016
Maximum	1.00	1.00	–

(15). The three-tank system was also simulated at the anticipated uncertainty of Table 1 to observe the most likely FDI performance and is shown in Fig. 3. In addition to the simulated tank heights, Figs. 2 and 3 display the tank height constraint plotted as the black solid line, the updated constraint for the 'Conservative' design plotted as the black dashed line, and the ranges of each tank height due to different realizations of uncertainty plotted as dotted lines filled in with the corresponding fault scenario color. Looking at the outputs for the worst-case realization of uncertainty in Fig. 2, the 'Nominal' design shows little to no separation in the 4 fault scenarios for all three of its outputs. The reason for this is that at these 'Nominal' conditions uncertainty causes the fault scenarios to be indistinguishable from each other. This is problematic when diagnosing the system for faults, as false alarms will be triggered when a fault-free system is mistaken to be one of the other fault scenarios. Even worse, this lack of separation can result in nondetections when a fault is present and the system is mistakenly assumed to be fault-free. The 'Mean' design shows significant improvement in separation over the 'Nominal' design, but the ranges of the Fault-Free and Tank 2 Leak scenarios violate the tank height constraint in Tanks 1 & 3. This is because the 'Mean' BIT was designed to satisfy the constraint at the anticipated uncertainty and did not account for other realizations of uncertainty. Fig. 3 illustrates this, as the simulated output of the 'Mean' design at the anticipated uncertainty lies on the tank height constraint for Tank 1. The 'Conservative' design fixes this problem by satisfying the updated tank height constraint, which is a buffer to the actual tank height constraint for potential deviations in tank height due to other realizations of uncertainty. However, this design underperforms in terms of FDI as there is still space before the actual tank height constraint is active that can be utilized for additional separation. The 'Worst-Case' design tackles this issue, as the actual constraint is active for the realization of uncertainty that occurs at the upper bound of its range. In this 'Worst-Case' FDI test, all three outputs of the 4 fault scenarios have adequate separation for the purposes of detection and isolation and adhere to the system tank height constraints for all realizations of uncertainty.

The objective function, calculated as the euclidean distance between all of the fault scenarios, is shown in Fig. 4 at the worst-case realization of uncertainty for each design. The bottom axes of Fig. 4 are the pump flow rates; the black solid line depicts the tank height constraint, indicating that for inputs above this line a realization of uncertainty exists that violates this constraint; and the red xy-plane through $z = 0$ indicates SIP feasibility, above which designs satisfy the semi-infinite constraint of (17). It is important to note that following the max-min inequality, the result shown in Fig. 4 is a lower bound of the feasible region. Looking simply at the surface of this lower bound, the objective function seems to be convex, verifying the assumption made on convexity for Algorithm 1. Therefore, Algorithm 1 can be used in this case for a computationally efficient robust FDI design. This does not reduce the significance of global methods, such as those described earlier. Global methods are important and necessary for providing rigorous guarantees to safety-critical applications, especially in systems where the FDI problem is nonconvex. For these problems, global methods are capable of overcoming localities to find improved BIT designs that local solvers cannot converge to. The global method of Algorithm 2 used in this work converged to the same solution as Algorithm 1 and confirms its SIP-feasibility, guaranteeing the robust BIT design.

When looking at the 'Worst-Case' design point in Fig. 4, it is clear why both inputs did not reach their interval bounds, as the design lies on the tank height constraint at the lower bound of input 2 and altering input 1 would degrade the FDI performance or violate the tank height constraint. Adjusting the physical system design by increasing the tank height or widening the input bounds would allow the inputs to be altered further and improve the FDI performance. For example, if no tank height constraint was present (i.e., the tanks were sufficiently large) then the greatest performing BIT of Fig. 4 lies at the upper bounds of inputs 1 and 2. The 'Worst-Case' design is the only design that satisfies both SIP feasibility (i.e., lies above the SIP feasible plane) and the system constraint.

Figs. 5(a)–(d) display the data of each fault scenario used to train the k-NN classifier. This data was obtained by running 10,000 Monte Carlo simulations with the normally distributed parameters in Table 1. Each of these 3-D plots shows a clearer view of how much overlap occurs between the fault scenarios at different realizations of uncertainty. A common occurrence between designs, exaggerated the most in Fig. 5(a), is the overlap between the fault-free and the Tank 2 leak (Fault 2) scenarios and the Pump 1 degradation (Fault 1) and the simultaneous (Fault 3) scenarios. The main cause of this is that for the Tank 2 leak scenario, the radius of the leak hole becomes minimal for some realizations of uncertainty, resulting in Fault 2 mimicking the fault-free scenario and Fault 3 mimicking the Fault 2 scenario. Furthermore, the 3-D plots also

Table 3
Respective worst-case realizations of uncertainty for the three-tank system BIT designs studied in Table 2.

Uncertain parameters	Min	Nominal	Mean	Conservative	Worst-case	Max
$\theta_{u,1}^*$ $(-)$	0.85	1.15	1.15	1.15	1.15	1.15
$\theta_{u,2}^*$ $(-)$	0.65	0.95	0.95	0.95	0.95	0.95
$\theta_{u,3}^*$ $(-)$	0.85	1.15	1.15	1.15	1.15	1.15
$\theta_{f,1}^*$ $(-)$	0.54	0.66	0.66	0.66	0.66	0.66
$\theta_{f,2}^*$ (m)	0.0005	0.0008	0.0018	0.0017	0.0018	0.005

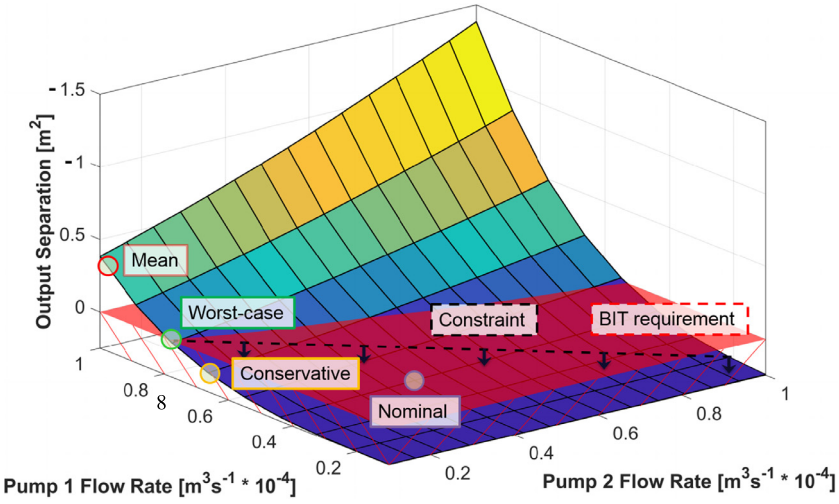
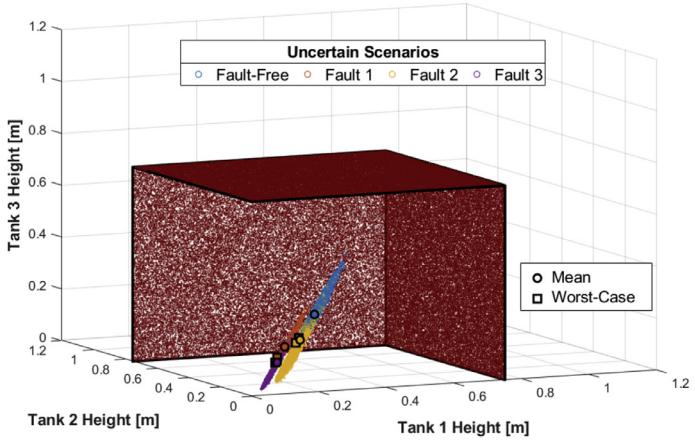
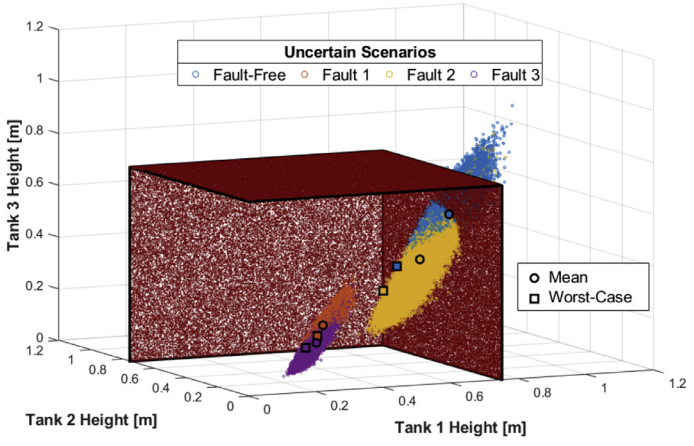


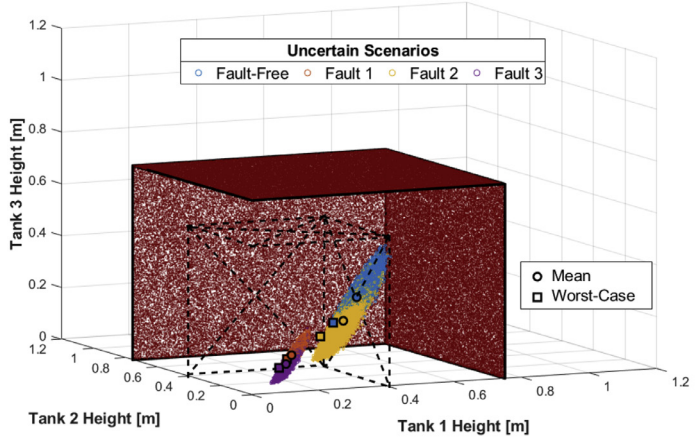
Fig. 4. The upper bound of program (17) showing the objective function (16), G, calculated for the worst-case realization of uncertainty without consideration of the state constraint. The red xy-plane at z=0 displays the SIP feasible region of FDI performance, where any point laying on or above it signifies a satisfactory worst-case BIT design. The black dotted line represents the tank height constraint, where any point on or below it signifies the constraint is satisfied. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)



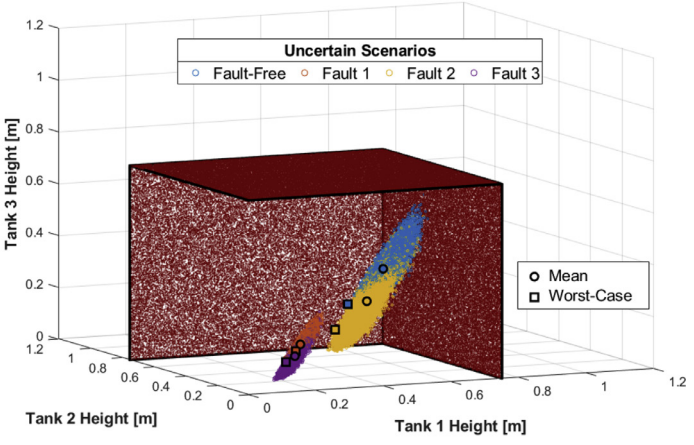
(a) 'Nominal' BIT design.



(b) 'Mean' BIT design.



(c) 'Conservative' BIT design.



(d) 'Worst-Case' BIT design.

Fig. 5. Steady state tank heights for 10,000 realizations of uncertainty (i.e., 40,000 data points given 4 fault scenarios) used to train k-NN classification. The axes indicate the heights of Tanks 1, 2, and 3. The individual circles represent the tank heights for a given realization of uncertainty at each fault scenario: blue corresponding to fault-free, red corresponding to Pump 1 degradation, yellow corresponding to Tank 2 leak, and purple corresponding to simultaneous faults. The bold circles and squares indicate the mean/anticipated and worst-case realizations of uncertainty, respectively. The red planes indicate the actual tank height constraint. The black dashed lines indicate the updated tank height constraint of the 'Conservative' BIT design. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

Table 4
Confusion matrices with equal weighted sensor fusion and a k-NN value of 21.

Design: Nominal, $A_{cc} = 0.7040$

		Actual			
		$c^{[0]}$	$c^{[1]}$	$c^{[2]}$	$c^{[3]}$
Predicted	$\hat{c}^{[0]}$	**0.93**	0.00	0.22	0.00
	$\hat{c}^{[1]}$	0.00	**0.85**	0.29	0.24
	$\hat{c}^{[2]}$	0.07	0.10	**0.28**	0.01
	$\hat{c}^{[3]}$	0.00	0.05	0.21	**0.75**

Design: Mean, $A_{cc} = 0.8452$

		Actual			
		$c^{[0]}$	$c^{[1]}$	$c^{[2]}$	$c^{[3]}$
Predicted	$\hat{c}^{[0]}$	**0.94**	0.00	0.23	0.00
	$\hat{c}^{[1]}$	0.00	**0.93**	0.00	0.24
	$\hat{c}^{[2]}$	0.06	0.00	**0.76**	0.00
	$\hat{c}^{[3]}$	0.00	0.07	0.01	**0.76**

Design: Conservative, $A_{cc} = 0.8273$

		Actual			
		$c^{[0]}$	$c^{[1]}$	$c^{[2]}$	$c^{[3]}$
Predicted	$\hat{c}^{[0]}$	**0.92**	0.00	0.24	0.00
	$\hat{c}^{[1]}$	0.00	**0.90**	0.00	0.27
	$\hat{c}^{[2]}$	0.08	0.01	**0.76**	0.00
	$\hat{c}^{[3]}$	0.00	0.09	0.00	**0.73**

Design: Worst-Case, $A_{cc} = 0.8377$

		Actual			
		$c^{[0]}$	$c^{[1]}$	$c^{[2]}$	$c^{[3]}$
	$\hat{c}^{[0]}$	**0.93**	0.00	0.24	0.00
	$\hat{c}^{[1]}$	0.00	**0.92**	0.00	0.29
	$\hat{c}^{[2]}$	0.07	0.01	**0.76**	0.00
	$\hat{c}^{[3]}$	0.00	0.07	0.00	**0.74**

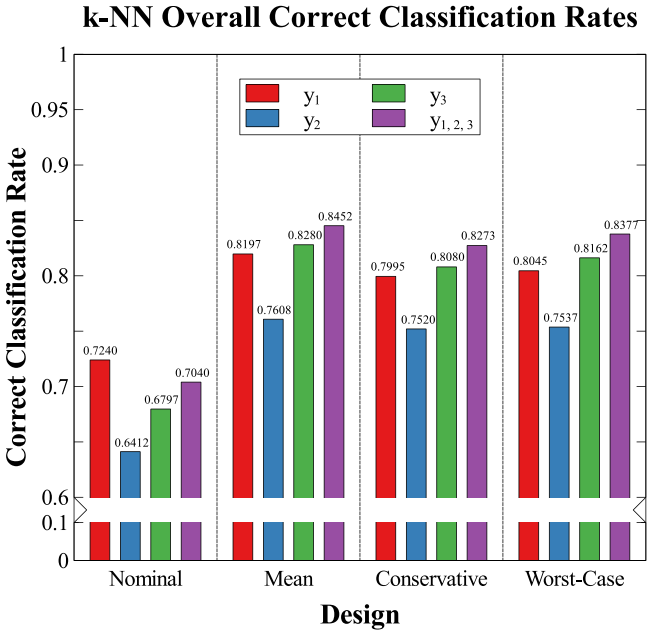


Fig. 6. Classification rates of each BIT design calculated from (13).

provide a clearer view of the tank height constraint violations that occur in the 'Mean' design and how the updated constraint of the 'Conservative' design helps solve this issue. The 'Worst-Case' design improves upon the 'Conservative' design by exploring the entire state domain, which activates but not violates the actual tank height constraint at a single realization of uncertainty.

After the k-NN classifier was trained, 1000 additional Monte Carlo simulation test data were generated to cross-validate the classifier in accordance to its overall accuracy and analyze the number of false alarms, nondetections, and incorrect classifications. Several values of $k \in \{1, 3, \ldots, 21\}$ were tested and compared, with $k = 21$ chosen because it produced the highest correct classification rate in the validation test data set. Alternatively, other methods of cross-validation such as the more thorough k-fold cross-validation can be utilized to better tune the number of neighbors used in classification (Mullin and Sukthankar, 2000). A confusion matrix was created that quantifies these events and is shown in Table 4. Each column in Table 4 denotes the simulated test class and each row denotes the estimated class from the k-NN classifier (12). The elements of Table 4 correspond to the percentage of tests that were calculated to belong to that class, with the diagonal elements reporting the percentage of correct classifications. For example, 93% of the fault-free tests ($c^{[0]}$) at the 'Worst-Case' design were correctly estimated as $\hat{c}^{[0]}$, leading to a 7% false alarm rate with the remaining tests estimated as the Tank 2 leak ($\hat{c}^{[2]}$). As expected from the overlap of fault scenarios shown earlier, most of the incorrect classifications in Table 4 occur for the Tank 2 leak ($c^{[2]}$) and the simultaneous ($c^{[3]}$) fault scenarios. The Tank 2 leak scenario has a 24% nondetection rate where it is incorrectly classified as the fault-free scenario $\hat{c}^{[0]}$. The simultaneous fault scenario has a 29% misclassification rate where it is incorrectly classified as the Pump 1 degradation scenario $c^{[1]}$. The overall correct classification rates of each FDI test design were calculated using (13) and are shown in Fig. 6. The classification rate for each of the individual outputs is shown next to the combined majority vote classification rate. As expected, the ranking of FDI test designs in terms of correct classification rates coincides with their objective function ranking, with the best performing FDI test design being the 'Mean' and the worst performing being the 'Nominal'. However, enforcing that the system constraints are met for all realizations of uncertainty, the 'Worst-Case' FDI test design provides the best possible correct classification rate.

4. Conclusions

We presented a method for the design of robust maintenance tests using local and global optimization of the admissible system inputs subject to constraints relating to the worst-case realization of uncertainty. The semi-infinite program presented was shown to be robust to all realizations of uncertainty. The global solution to this problem provides certifiable guarantees valuable in application to safety-critical systems. This problem was solved locally using the Blankenship and Falk cutting plane algorithm (Blankenship and Falk, 1976) presented by Asprey and Macchietto (2002) and its SIP feasibility was confirmed globally using a cutting plane algorithm presented by Stuber and Barton (2015). The method and programs developed were applied on the three-tank benchmark system. Several FDI test designs were compared to the SIP-optimal 'Worst-Case' test design. The SIP-optimal test was capable of distinguishing between a fault-free system and three separate fault scenarios, which was not possible with a 'Nominal' test. The 'Worst-Case' FDI test also satisfied the system safety constraint that other designs violated while performing at its best possible feasible point. This was illustrated *a posteriori* using k-NN classification with the 'Worst-Case' FDI test design having higher correct classification rates than both the 'Nominal' and 'Conservative' designs.

Acknowledgments

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.

References

Ashari, A.E., Nikoukhah, R., Campbell, S.L., 2012. Effects of feedback on active fault detection. Automatica 48 (5), 866–872. doi:10.1016/j.automatica.2012.02.020.

Asprey, S.P., Macchietto, S., 2002. Designing robust optimal dynamic experiments. J. Process Control 12 (4), 545–556.

Belcastro, C.M., 2011. Aircraft loss of control: Analysis and requirements for future safety-critical systems and their validation. In: 2011 8th Asian Control Conference (ASCC), pp. 399–406.

Bezanson, J., Edelman, A., Karpinski, S., Shah, V.B., 2017. Julia: a fresh approach to numerical computing. SIAM Rev. 59 (1), 65–98. doi:10.1137/141000671.

Bhattacharjee, B., Lemonidis, P., Green Jr., W.H., Barton, P.I., 2005. Global solution of semi-infinite programs. Math. Program. 103 (2), 283–307. doi:10.1007/s10107-005-0583-6.

Blankenship, J.W., Falk, J.E., 1976. Infinitely constrained optimization problems. J. Optim. Theory Appl. 19 (2), 261–281.

Bollas, G.M., Barton, P.I., Mitsos, A., 2009. Bilevel optimization formulation for parameter estimation in vapor–liquid (–liquid) phase equilibrium problems. Chem. Eng. Sci. 64 (8), 1768–1783.

DeCock, A., Gevers, M., Schoukens, J., 2016. D-Optimal input design for nonlinear FIR-type systems: a dispersion-based approach. Automatica 73, 88–100.

Falk, J.E., Hoffman, K., 1977. A nonconvex max-min problem. Naval Res. Logist. Q. 24 (3), 441–450.

Fekih, A., 2014. Fault diagnosis and Fault Tolerant Control design for aerospace systems: a bibliographical review. In: Proceedings of 2014 Annual American Control Conference (ACC). Portland, Oregon, pp. 1286–1291. doi:10.1109/ACC.2014.6859271.

Floudas, C.A., Gounaris, C.E., 2009. A review of recent advances in global optimization. J. Global Optim. 45, 3–38.

Floudas, C.A., Gümüş, Z.H., Ierapetritou, M.G., 2001. Global optimization in design under uncertainty: feasibility test and flexibility index problems. Ind. Eng. Chem. Res. 40 (20), 4267–4282. doi:10.1021/ie001014g.

Gajjar, S., Kulahci, M., Palazoglu, A., 2018. Real-time fault detection and diagnosis using sparse principal component analysis. J. Process Control 67, 112–128. doi:10.1016/j.jprocont.2017.03.005.

Hale, W.T., Bollas, G.M., 2018. Design of built-In tests for active fault detection and isolation of discrete faults. IEEE Access 6, 50959–50973. doi:10.1109/access.2018.2869269.

Hale, W.T., Palmer, K.A., Stuber, M.D., Bollas, G.M., 2018. Design of built-in tests for robust active fault detection and isolation of discrete faults in uncertain systems. In: Proceedings of 2018 Annual American Control Conference (ACC). Milwaukee, Wisconsin, pp. 4989–4994. doi:10.23919/ACC.2018.8431233.

Halemane, K.P., Grossmann, I.E., 1983. Optimal process design under uncertainty. AIChE J. 29 (3), 425–433. doi:10.1002/aic.690290312.

Hettich, R., Kortanek, K.O., 1993. Semi-infinite programming: theory, methods, and applications. SIAM Rev. 35 (3), 380–429.

Hwang, I., Kim, S., Kim, Y., Seah, C.E., 2010. A survey of fault detection, isolation, and reconfiguration methods. IEEE Trans. Control Syst. Technol. 18 (3), 636–653.

Khan, S., Phillips, P., Hockley, C., Jennions, I., 2014. No fault found events in maintenance engineering part 2: root causes, technical developments and future research. Reliab. Eng. Syst. Saf. 123, 196–208.

Khan, S., Phillips, P., Jennions, I., Hockley, C., 2014. No fault found events in maintenance engineering part 1: current trends, implications and organizational practices. Reliab. Eng. Syst. Saf. 123, 183–195.

Kim, M.H., Lee, S., Lee, K.C., 2010. Kalman predictive redundancy system for fault tolerance of safety-Critical systems. IEEE Trans. Ind. Inf. 6 (1), 46–53. doi:10.1109/tii.2009.2020566.

Kwak, B.M., Haug, E.J., 1976. Optimum design in the presence of parametric uncertainty. J. Optim. Theory Appl. 19 (4), 527–546. doi:10.1007/bf00934653.

Mesbah, A., Streif, S., Findeisen, R., Braatz, R.D., 2014. Active fault diagnosis for nonlinear systems with probabilistic uncertainties. IFAC Proc. Volumes 47 (3), 7079–7084.

Mitsos, A., 2011. Global optimization of semi-infinite programs via restriction of the right-hand side. Optimization 60 (10–11), 1291–1308.

Mitsos, A., Bollas, G.M., Barton, P.I., 2009. Bilevel optimization formulation for parameter estimation in liquid–liquid phase equilibrium problems. Chem. Eng. Sci. 64 (3), 548–559.

Mitsos, A., Lemonidis, P., Barton, P.I., 2007. Global solution of bilevel programs with a nonconvex inner program. J. Global Optim. 42 (4), 475–513. doi:10.1007/s10898-007-9260-z.

Moosavian, A., Ahmadi, H., Tabatabaeefar, A., Khazaee, M., 2013. Comparison of two classifiers; K-nearest neighbor and artificial neural network, for fault diagnosis on a main engine journal-bearing. Shock Vib. 20 (2), 263–272. doi:10.3233/SAV-2012-00742.

Mullin, M., Sukthankar, R., 2000. Complete cross-validation for nearest neighbor classifiers. In: 17th International Conference on Machine Learning (ICML), pp. 1–8.

Najjar, N., Gupta, S., Hare, J., Kandil, S., Walthall, R., 2016. Optimal sensor selection and fusion for heat exchanger fouling diagnosis in aerospace systems. IEEE Sens. J. 16 (12), 4866–4881. doi:10.1109/JSEN.2016.2549860.

Niemann, H., 2006. A setup for active fault diagnosis. IEEE Trans. Autom. Control 51 (9), 1572–1578. doi:10.1109/TAC.2006.878724.

Onel, M., Kieslich, C.A., Guzman, Y.A., Floudas, C.A., Pistikopoulos, E.N., 2018. Big data approach to batch process monitoring: simultaneous fault detection and diagnosis using nonlinear support vector machine-based feature selection. Comput. Chem. Eng. 115, 46–63. doi:10.1016/j.compchemeng.2018.03.025.

Onel, M., Kieslich, C.A., Guzman, Y.A., Pistikopoulos, E.N., 2018. Simultaneous Fault Detection and Identification in Continuous Processes via Nonlinear Support Vector Machine Based Feature Selection. In: Eden, M.R., Ierapetritou, M.G., Towler, G.P. (Eds.), 13th International Symposium on Process Systems Engineering (PSE 2018). In: Computer Aided Chemical Engineering, 44. Elsevier BV, pp. 2077–2082. doi:10.1016/B978-0-444-64241-7.50341-4.

Ossmann, D., 2014. Optimization based tuning of fault detection and diagnosis systems for safety critical systems. IFAC Proc. Volumes 47 (3), 8570–8575. doi:10.3182/20140824-6-za-1003.00159.

Palmer, K.A., Bollas, G.M., 2018. Analysis of transient data in test designs for active fault detection and identification. Comput. Chem. Eng. (in press) 1–12. doi:10.1016/j.compchemeng.2018.06.020.

Palmer, K.A., Bollas, G.M., 2019. Active fault diagnosis for uncertain systems using optimal test designs and detection through classification. ISA Trans. (in press) 1–16. doi:10.1016/j.isatra.2019.02.034.

Palmer, K.A., Hale, W.T., Bollas, G.M., 2018. Active fault identification by optimization of test designs. IEEE Trans. Control Syst. Technol. (in pess) 1–15. doi:10.1109/TCST.2018.2867996.

Palmer, K.A., Hale, W.T., Such, K.D., Shea, B.R., Bollas, G.M., 2016. Optimal design of tests for heat exchanger fouling identification. Appl. Therm. Eng. 95, 382–393. doi:10.1016/j.applthermaleng.2015.11.043.

Puschke, J., Djelassi, H., Kleinekorte, J., Hannemann-Tamás, R., Mitsos, A., 2018. Robust dynamic optimization of batch processes under parametric uncertainty: utilizing approaches from semi-infinite programs. Comput. Chem. Eng. doi:10.1016/j.compchemeng.2018.05.025.

Saha, S., Sadi, M.S., 2012. Synthesizing fault tolerant safety critical systems. In: 2012 15th International Conference on Computer and Information Technology (ICCIT), pp. 452–457. doi:10.1109/iccitechn.2012.6509720.

Scott, J.K., Findeisen, R., Braatz, R.D., Raimondo, D.M., 2013. Design of active inputs for set-based fault diagnosis. In: Proceedings of 2013 Annual American Control Conference (ACC), pp. 3561–3566.

Shahnazari, H., Mhaskar, P., House, J.M., Salsbury, T.I., 2018. Heating, ventilation and air conditioning systems: fault detection and isolation and safe parking. Comput. Chem. Eng. 108, 139–151. doi:10.1016/j.compchemeng.2017.08.012.

da Silva, J.C., Saxena, A., Balaban, E., Goebel, K., 2012. A knowledge-based system approach for sensor fault modeling, detection and mitigation. Expert Syst. Appl. 39 (12), 10977–10989. doi:10.1016/j.eswa.2012.03.026.

Streif, S., Hast, D., Braatz, R.D., Findeisen, R., 2013. Certifying robustness of separating inputs and outputs in active fault diagnosis for uncertain nonlinear systems. IFAC Proc. Volumes 46 (32), 837–842. 10th IFAC International Symposium on Dynamics and Control of Process Systems.

Stuber, M.D., Barton, P.I., 2011. Robust simulation and design using semi-infinite programs with implicit functions. Int. J. Reliab. Saf. 5 (3/4), 378. doi:10.1504/ijrs.2011.041186.

Stuber, M.D., Barton, P.I., 2015. Semi-infinite optimization with implicit functions. Ind. Eng. Chem. Res. 54, 307–317.

Stuber, M.D., Scott, J.K., Barton, P.I., 2015. Convex and concave relaxations of implicit functions. Optim. Methods Softw. 30 (3), 424–460. doi:10.1080/10556788.2014.924514.

Stuber, M.D., Wechsung, A., Sundaramoorthy, A., Barton, P.I., 2014. Worst-case design of subsea production facilities using semi-infinite programming. AIChE J. 60 (7), 2513–2524.

Swaney, R.E., Grossmann, I.E., 1985. An index for operational flexibility in chemical process design. part II: computational algorithms. AIChE J. 31 (4), 631–641. doi:10.1002/aic.690310413.

Šimandl, M., Punčochář, I., 2009. Active fault detection and control: unified formulation and optimal design. Automatica 45 (9), 2052–2059. doi:10.1016/j.automatica.2009.04.028.

Tamura, M., Tsujita, S., 2007. A study on the number of principal components and sensitivity of fault detection using PCA. Comput. Chem. Eng. 31 (9), 1035–1046. doi:10.1016/j.compchemeng.2006.09.004.

Venkatasubramanian, V., Rengaswamy, R., Yin, K., Kavuri, S.N., 2003. A review of process fault detection and diagnosis: part i: quantitative model-based methods. Comput. Chem. Eng. 27 (3), 293–311. doi:10.1016/s0098-1354(02)00160-6.

Walz, O., Djelassi, H., Caspari, A., Mitsos, A., 2018. Bounded-error optimal experimental design via global solution of constrained min–max program. Comput. Chem. Eng. 111, 92–101. doi:10.1016/j.compchemeng.2017.12.016.

Wilhelm, M. E., Stuber, M. D.,. Easy Advanced Global Optimization (EAGO): an open-source platform for robust and global optimization. https://github.com/PSORLab/EAGO.jl. Online; accessed June, 2018.

Wisniewski, R., Svenstrup, M., Pedersen, A.S., Steiniche, C.S., 2013. Certificate for safe emergency shutdown of wind turbines. In: Proceedings of 2013 Annual American Control Conference (ACC), pp. 3667–3672. doi:10.1109/acc.2013.6580399.

Yu, J., 2013. A support vector clustering-based probabilistic method for unsupervised fault detection and classification of complex chemical processes using unlabeled data. AIChE J. 59 (2), 407–419. doi:10.1002/aic.13816.