Reachability Analysis as a Design Tool for Stormwater Systems

Margaret P. Chapman[1], Kevin M. Smith[2], Victoria Cheng[3], David L. Freyberg[4], and Claire J. Tomlin[1]

Abstract— **Effective stormwater management requires systems that operate safely and deliver improved environmental outcomes in a cost-effective manner. However, current design practices typically evaluate performance assuming that a given system starts empty and operates independently from nearby stormwater infrastructure. There is a conspicuous need for more realistic design-phase indicators of performance that consider a larger set of initial conditions and the effects of coupled dynamics. To this end, we apply a control-theoretic method, called *reachability analysis*, to produce a more objective measure of system robustness. We seek two primary contributions in this work. First, we demonstrate how the application of reachability analysis to a dynamic model of a stormwater network can characterize the set of initial conditions from which every element in the network can avoid overflowing under a given surface runoff signal of finite duration. This is, to the authors' knowledge, the first published application of reachability analysis to stormwater systems. Our second contribution is to offer an interpretation of the outcomes of the proposed reachability analysis as a measure of system robustness that can provide useful information when making critical design decisions. We illustrate the effectiveness of this method in revealing the trade-offs of particular design choices relative to a desired level of robustness.**

I. Premise

A stormwater system is a network of infrastructure and natural topology that is designed to manage excess water from rainfall or snowmelt that accumulates near developed areas. In the United States, stormwater systems are subject to federal regulation, namely the National Pollutant Discharge Elimination System permit program [1]. Stormwater permitting is administered in ways that give substantial flexibility to regional and municipal governments in pursuing compliance. Stormwater systems, as a result, vary widely and are designed to meet local needs for flood control, erosion mitigation, or pollutant capture. A primary design criterion common to most regulatory contexts is that a new stormwater system must accommodate an extreme synthetic storm, known as a design storm, if the system starts empty. Further, a new element of stormwater infrastructure, such as a detention pond, is typically designed as an isolated entity even if it will be linked to elements that are present nearby. These standard design practices provide limited information about the performance of stormwater systems under realistic operating conditions, where systems may not be empty at the start of storm events and typically do not operate in isolation from one another.

In this paper, we propose the use of a control-theoretic method, called *reachability analysis*, to provide a design-phase indicator of system performance under more realistic operating conditions. Reachability analysis can augment existing design practices with valuable insight into how a given system behaves starting from a comprehensive set of physically realizable initial conditions without the need for independent simulations.[1] In addition, reachability analysis encodes how the behavior of an element of the system affects the behavior of another element, and conveys these effects quantitatively as well as qualitatively. A designer could use reachability analysis to evaluate the impact of modifying infrastructure more realistically than what is permitted by standard methods, and to select interventions that facilitate safer and more effective operation of the system in practice.

This paper demonstrates the application of reachability analysis as a design tool for stormwater infrastructure. We provide an illustration of how this technique could inform retrofit options for an existing two-pond stormwater network in Lenexa, Kansas (Fig. 1). These two ponds are connected in series and have valves that can be actuated for real-time control. We note that the broader class of multi-reservoir optimization and control problems have been of interest to the hydrology community over the past several decades (see, for example, [5] and the references therein), but no hydrology publications, to the authors' knowledge, have utilized the reachability techniques that we describe. Sec. II presents reachability analysis in the context of quantifying the robustness of stormwater systems. In this section, we explain what reachability analysis is, present a dynamic model of our system, exemplify how reachability analysis indicates system behavior, and propose metrics of system robustness. Sec. III builds on the previous examples to show how reachability analysis can be used to inform safety-critical design choices. Sec. IV concludes the paper with plans for future work.

II. Process

A. Reachability Analysis

Reachability analysis is a formal verification method based on the theories of optimal control and dynamic games that

[1]M.C. and C.T. are with the Department of Electrical Engineering and Computer Sciences, University of California at Berkeley, USA. chapmanm@berkeley.edu

[2]K.S. is with OptiRTC, Inc. and the Department of Civil and Environmental Engineering, Tufts University, USA.

[3]V.C. is with the Department of Civil and Environmental Engineering, University of California at Berkeley, USA.

[4]D.F. is with the Department of Civil and Environmental Engineering, Stanford University, USA.

[1] The reachability method that we apply here uses a Hamilton-Jacobi formulation of dynamic programming to implicitly compute the outcomes of the paths that the system can follow in a discretized state space (i.e., grid) [2], [3], [4]. An example outcome of a given path is whether the system satisfies its constraints while it traverses the path.

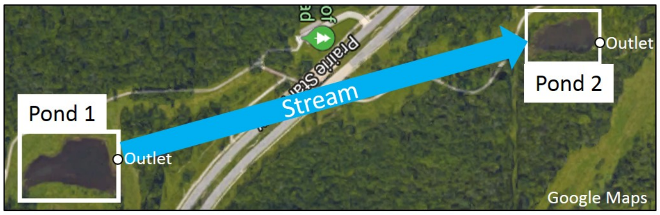

Fig. 1. A photo of a stormwater system in Lenexa, Kansas that consists of two ponds in series (Google Maps).

is used to guarantee the performance and safety of dynamic systems [4]. Reachability analysis has been widely applied to the control of vehicles (e.g., see [2], [6], and [7]) due to the availability of sufficiently low-dimensional vehicle models and the need for vehicles to satisfy guarantees in performance (e.g., reach a given destination) and safety (e.g., avoid collisions). In this paper, we use reachability analysis to quantify the robustness of stormwater infrastructure in order to inform critical design decisions. To our knowledge, this paper is the first published application of reachability analysis to stormwater systems.

Given a dynamic system *model*, a *constraint set*, and a *time horizon*, reachability analysis can provide the set of initial states from which the system is guaranteed to stay inside the constraint set during the time horizon. This set of initial states is called the *safe set*. The safe set is a measure of the system's robustness because it captures the ability of the system to operate satisfactorily, starting from a range of initial conditions (e.g., initial pond stage), while subject to external disturbances (e.g., surface runoff).

B. Dynamic System Model

In this paper, the dynamic system is the flow of water through two ponds connected in series via a stream, as shown in Fig. 1. The dynamic system model is a simplified abstraction of the actual system, shown in Fig. 2, that describes how the stages of the ponds (x_1, x_3) and the stage of the stream (x_2) change over time in response to surface runoff (d_1, d_2) and the positions of the valves (u_1, u_2) which control discharge from the ponds. Note that $u_i = 0$ means that the valve of pond i is fully closed, whereas $u_i = 1$ means that the valve of pond i is fully open. The *state* of the system is $x = [x_1, x_2, x_3]^T \in \mathbb{R}^3$, where each x_i has units of feet. The *controls* are u_1 and u_2, which are unitless, and we introduce the vector, μ, as the corresponding *control signal*, $\mu(t) = [u_1(t), u_2(t)]^T$. Since we will consider scenarios in which u_1 and u_2 change over time, μ is generally represented as a function of time. The *disturbances* are d_1 and d_2, which have units of cubic feet per second (cfs), and we introduce the vector, γ, as the corresponding *disturbance signal*, $\gamma(t) = [d_1(t), d_2(t)]^T$. Since we will consider scenarios in which d_1 and d_2 change over time, γ is generally represented as a function of time. The dynamic system model is a system of coupled ordinary differential equations derived from the principles of hydraulics,

$$\dot{x}_1 = \frac{d_1 - q_p(x_1, u_1)}{A_1} \tag{1a}$$

$$\dot{x}_2 = \frac{q_p(x_1, u_1) - q_s(x_2)}{a_s(x_2)} \tag{1b}$$

$$\dot{x}_3 = \frac{q_s(x_2) + d_2 - q_p(x_3, u_2)}{A_2}, \tag{1c}$$

where pond outflow, q_p (units in cfs), is described by the orifice equation,

$$q_p(x, u) = \begin{cases} C_d \pi R^2 u \sqrt{2g(x - Z)} & \text{if } x \geq Z \\ 0 & \text{if } x < Z, \end{cases} \tag{2}$$

and stream outflow, q_s (units in cfs), is described by Manning's open channel flow equation,

$$q_s(x_2) = \begin{cases} a_f(x_2) \cdot R_h(x_2)^{2/3} \cdot \frac{1.486\sqrt{S}}{n} & \text{if } x \geq Y \\ 0 & \text{if } x < Y. \end{cases} \tag{3}$$

The terms in the preceding equations are defined in Table I. After several iterations, we chose (1)-(3) because these equations are simple enough to illustrate reachability analysis, a computational technique that is new to the stormwater community, and these equations are based on well-established hydraulics principles. We primarily used [8] and [9] to formulate (1)-(3). Revision and validation of the model is reserved for future work, as the purpose of the current paper is the application of reachability analysis to inform safety-critical design choices for stormwater infrastructure.

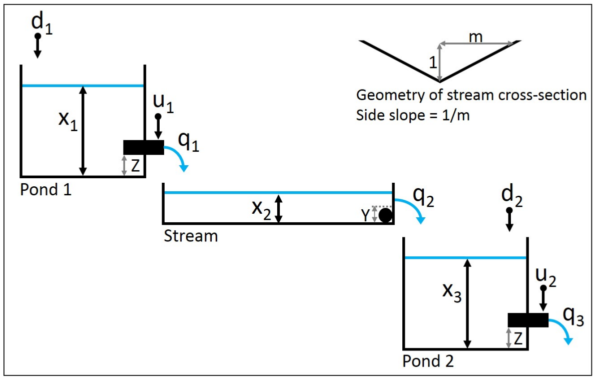

Fig. 2. A low-dimensional model of a stormwater system that consists of two ponds connected in-series via a stream. The dynamics equations are given by (1)-(3). The outflow from pond 1 is $q_1 := q_p(x_1, u_1)$. The outflow from the stream is $q_2 := q_s(x_2)$, and the outflow from pond 2 is $q_3 := q_p(x_3, u_2)$. For simplicity, the stream is assumed to be straight with a triangular cross-section, and the surface area of each pond is assumed to be constant. The system dynamics assume that evaporation effects are negligible and that all surface runoff flows into one of the two ponds.

C. Computational Software

In this paper, all reachability computations were performed using the Level Set Toolbox [10] and the Hamilton-Jacobi Optimal Control Toolbox [11] in MATLAB.[2] Watershed

[2] MATLAB R2016b, The MathWorks, Inc., Natick, MA.

delineation and rainfall-runoff simulations were performed using PCSWMM.[3]

D. Numerical Examples

In this section, we present numerical examples of reachability analysis so the reader can build intuition for interpreting safe sets. Informally, the safe set is the set of initial states from which the system will satisfy the constraints over the time horizon, assuming that the dynamics of the system behave according to a model with certain properties.[4] In this paper, satisfying the constraints means that the system does not overflow, a condition that could lead to flooding and catastrophic embankment failure. We characterize the avoidance of overflow through the use of a constraint set, $\mathcal{K}$,

$$\mathcal{K} := \{x \in \mathbb{R}^3 \mid 0 < x_i \leq X_i \text{ for each } i\}, \tag{4}$$

where $X_1 = 5$ ft, $X_2 = 3$ ft, and $X_3 = 3.5$ ft, which are estimates derived from an existing stormwater network in Lenexa, Kansas. In this paper, we use a time horizon of four hours in duration, $T = 4\text{h}$. Given control signal μ and disturbance signal γ, the safe set at time $t \in [0, T]$ is defined as,

$$\mathcal{S}(t; \mu, \gamma) := \{y \in \mathbb{R}^3 \mid \xi(\tau; y, t, \mu, \gamma) \in \mathcal{K} \ \forall \tau \in [t, T]\}, \tag{5}$$

where $\xi(\tau; y, t, \mu, \gamma)$ is the state at time τ starting from state y at time t, subject to the control signal μ, the disturbance signal γ, and the dynamic model (1).[5] Note that, for any control signal and disturbance signal, the safe set at time T is equal to $\mathcal{K}$.

TABLE I

Symbol	Definition	Value
A_1	Surface area of pond 1	28,292 ft^2
A_2	Surface area of pond 2	25,965 ft^2
$a_f(x_2)$	Flow cross-sectional area of stream as a function of stream stage	$a_f(x_2) = m(x_2)^2$ ft^2
$a_s(x_2)$	Surface area of stream as a function of stream stage	$a_s(x_2) = 2mx_2L$ ft^2
C_d	Discharge coefficient of outlet	0.61
g	Acceleration due to gravity	32.2 ft/s^2
L	Length of stream	$1,820$ ft
m	Inverse of stream side slope	4 horizontal ft per vertical ft
n	Manning's roughness coefficient	0.1 s/m$^{1/3}$
R	Radius of pond outlet	$1/3$ ft
$R_h(x_2)$	Hydraulic radius of stream as a function of stream stage	$r(x_2) = \frac{m}{2\sqrt{1+m^2}} x_2$ ft
S	Slope of stream	0.01 ft/ft
Y	Minimum stream stage	0.5 ft
Z	Elevation of pond outlet	1 ft

Parameters for the dynamic system model (1)-(3). We used [8], [9], and estimates based on the system in Lenexa, Kansas to obtain many of the above values.

1) Two-Dimensional Examples: Since three-dimensional sets are more challenging to interpret, we will first show examples of safe sets for the two-dimensional subsystem described by (1a) and (1b). In these examples, the constraint set is the projection of $\mathcal{K}$ onto $\mathbb{R}^2$,

$$\mathcal{K}' = \{x \in \mathbb{R}^2 \mid 0 < x_1 \leq 5, \ 0 < x_2 \leq 3\}. \tag{6}$$

For simplicity, we choose the control signal, μ, and the disturbance signal, γ, to be constant over time. Since the two-dimensional subsystem has one control and one disturbance, $\mu(t) = u_1$ and $\gamma(t) = d_1$, for all $t \in [0, 4\text{h}]$. Fig. 3 shows the safe sets for six distinct combinations of values for d_1 and u_1.

Scenario I: $d_1 = 0$, $u_1 = 0$ (Fig. 3, row 1, column 1). Any initial value for x_1 (pond stage) will not change over time because no water enters or leaves the pond. Recall that $u_1 = 0$ means the valve controlling the discharge from the pond is fully closed. So, if the pond stage starts between 0 and 5ft, it will continue to satisfy these constraints. Any initial value for x_2 (stream stage) that exceeds $Y = \frac{1}{2}$ft will decrease until $x_2 = Y$, and any initial value for x_2 that is smaller than Y will not change over time. So, if the stream stage starts between 0 and 3ft, it will continue to satisfy these constraints. The safe set for all $t \in [0, 4\text{h}]$ is equal to $\mathcal{K}'$.

Scenario II: $d_1 = 0$, $u_1 = 1$ (Fig. 3, row 1, column 2). If the initial value for x_1 is smaller than $Z = 1$ft, then no water will leave the pond, and the situation reduces to Scenario I. If the initial value for x_1 exceeds Z, then water will enter the stream, and x_1 will decrease until $x_1 = Z$. So, if the pond satisfies the constraints initially, it will continue to do so. If the stream were ever to overflow after the system starts within $\mathcal{K}'$, it would occur when x_1 and x_2 start maximally. Why? Higher pond stage implies faster flow rate into the stream, and if the stream starts full, then any increase in stream stage will cause overflow. But, even if $x_1 = 5$ft and $x_2 = 3$ft at time 0, then $\dot{x}_2$ becomes negative instantaneously, and x_2 will decrease. The flow rate out of the stream, $q_s(x_2)$, is much higher than the flow rate into the stream, $q_p(x_1, 1)$, at high stages; see (1b). This suggests that the stream cannot overflow if it initially satisfies the constraints.

Scenario III: $d_1 = 2$cfs, $u_1 = 0$ (Fig. 3, row 2, column 1). Surface runoff enters the pond at a constant rate for 4 hours, while the valve is closed. Since no water enters the stream, if the stream satisfies the constraints initially, then it will continue to do so. Observe that the boundary of the safe set at time 0 along the x_1-axis is at $x_1 = 4$ft, whereas this boundary is at $x_1 = 5$ft when $d_1 = 0$cfs (Scenario I). Why? The volume of water that enters the pond in total is 28,800ft^3, which is about equal to the surface area of the pond multiplied by 1ft (Table I). So, if x_1 starts above 4ft,

[3] PCSWMM Professional Edition, Version 7.1.2480, Computational Hydraulics International, Guelph, Ontario.

[4] The properties on the model that are required for reachability analysis are summarized nicely in [12], see Sec. 2.1, System Model.

[5] In reachability theory, safe sets are not usually parametrized by the control signal or the disturbance signal (e.g., see [4]). We use this parametrization, however, because the disturbance signal is fixed, and the control signal is often fixed, in our examples.

then the pond cannot retain all of the incoming water over the next 4 hours. However, if x_1 starts below 4ft, then the pond can retain all of the incoming water over the next 4 hours. We will explain the safe sets at time $t > 0$ when we discuss Scenario V.

Scenario IV: $d_1 = 2$cfs, $u_1 = 1$ (Fig. 3, row 2, column 2). The same amount of rain enters the pond over 4 hours, as in Scenario III, but now the valve is open. The safe set at time 0 is equal to $\mathcal{K}'$. Why? The pond outflow rate, q_p, equals the surface runoff rate, $d_1 = 2$cfs, when x_1 is about 2.4ft; see (2). $\dot{x}_1$ is proportional to $d_1 - q_p$; see (1a). So, if x_1 initially exceeds 2.4ft, then $\dot{x}_1$ will be negative, and x_1 will decrease until $q_p = d_1$. If x_1 starts smaller than 2.4ft, then $\dot{x}_1$ will be positive, and x_1 will increase until $q_p = d_1$. Thus, if x_1 starts between 0ft and 5ft, then the pond will continue to satisfy these constraints. Since the flow rate out of the stream is generally much larger than the flow rate into the stream, the safe set will not shrink along the x_2-axis.

Scenario V: $d_1 = 4$cfs, $u_1 = 0$ (Fig. 3, row 3, column 1). The safe set at time 0 is smaller than the safe set at time 20min. Why? The safe set at time 0 contains the states where the system can be at time 0, from which it will not overflow during the next 4 hours. The safe set at time 20min contains the states where the system can be at time 20min, from which it will not overflow during the next 3 hours and 40 minutes. 20 minutes of surface runoff entering the pond at 4cfs increases the stage of the pond by 0.17ft.[6] So, the safe set along the x_1-axis at time 0 is 0.17ft smaller than the safe set along the x_1-axis at time 20min. More generally, since the rate of surface runoff is constant, the safe set along the x_1-axis at time t is 0.17ft smaller than the safe set along the x_1-axis at time $t + 20$min, for all $t \in [0, 3\text{h } 40\text{min}]$.

Scenario VI: $d_1 = 4$cfs, $u_1 = 1$ (Fig. 3, row 3, column 2). As before, the safe set at time $t \in [0, 4\text{h}]$ extends from 0ft to 3ft along the x_2-axis because the flow rate out of the stream is generally much larger than the flow rate into the stream. Compare Scenarios V and VI, which have equal surface runoff rates. In Scenario V, the valve is closed, and the safe set at time 0 extends from 0ft to about 3ft along the x_1-axis. In Scenario VI, the valve is open, so the pond is able to release water, which increases the size of the safe set at time 0 along the x_1-axis. More generally, due to the open valve, the safe set at time t in Scenario VI is at least as large as the safe set at time t in Scenario V, for all $t \in [0, 4\text{h}]$. Compare Scenario VI with Scenario IV, which both have the valve open ($u_1 = 1$) for the duration. In Scenario IV, $d_1 = 2$cfs, which is less than the maximum obtainable discharge of pond 1, $q_p(5\text{ft}, 1) \approx 3.4$cfs, which yields a safe set at time 0 equal to $\mathcal{K}'$. For Scenario VI, in contrast, the constant disturbance, $d_1 = 4$cfs, exceeds the maximum obtainable discharge of pond 1, and therefore causes the safe set to be diminished for all $t < 4$h.

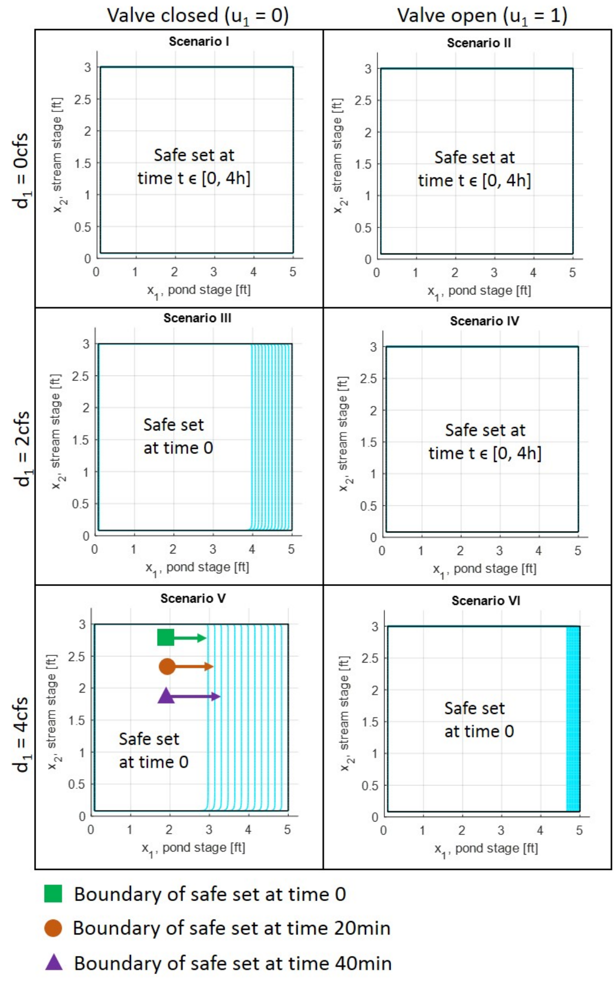

Fig. 3. Results from reachability analysis on the two-dimensional subsystem, described by (1a) and (1b), with constant control and disturbance signals, over a four-hour time horizon. The constraint set is $\mathcal{K}' = \{x \in \mathbb{R}^2 \mid 0 < x_1 \leq 5, 0 < x_2 \leq 3\}$. For each scenario, the smallest blue rectangle inside $\mathcal{K}'$ is the boundary of the safe set at time zero. The second blue smallest rectangle inside $\mathcal{K}'$ is the boundary of the safe set at time 20 minutes. The third smallest blue rectangle inside $\mathcal{K}'$ is the boundary of the safe set at time 40 minutes, etc.

2) Three-Dimensional Example: Now, we will study the safe set at time zero for the three-dimensional system given by (1a)-(1c), such that the surface runoff is zero and the valves are open over time. Formally, we choose the disturbance signal, $\gamma(t) = [d_1, d_2]^T = [0, 0]^T$, and the control signal, $\mu(t) = [u_1, u_2]^T = [1, 1]^T$, for all $t \in [0, 4\text{h}]$. Recall that this safe set is the set of all states at time zero from which the system will remain inside $\mathcal{K}$, see (4), over the time horizon, assuming the given model. This safe set is provided in Fig. 4, where approximate two-dimensional cross-sections are specified along each axis.

Consider Fig. 4a. As x_3 increases, the safe set extends shorter distances in the x_2-direction. For example, at $x_3 = 2$ft, the safe set extends to about 2.6ft in the x_2-direction (Fig. 4a, middle plane). At $x_3 = 3.4$ft, the safe set extends to about 1.2ft in the x_2-direction (Fig. 4a, top plane). If x_3 starts small, then pond 2 can accept large volumes of water

[6] The volume of water that enters the pond in 20 minutes is $4\frac{\text{ft}^3}{\text{s}} \cdot \frac{60\text{s}}{1\text{min}} \cdot 20\text{min} = 4,800\text{ft}^3$. Since the pond has a constant surface area of 28,292ft^2, the associated increase in stage is $\frac{4{,}800\text{ft}^3}{28{,}292\text{ft}^2} = 0.17$ft.

from the stream without overflowing. This situation is similar to Scenario II for the two-dimensional subsystem; compare Fig. 4a (bottom plane) and Fig. 3 (Scenario II). However, as the initial value of x_3 increases, pond 2 can only tolerate smaller volumes of water entering from the stream, since the flow rate out of the pond is typically much smaller than the flow rate into the pond.

Consider Fig. 4b. As x_2 increases, the safe set extends shorter distances in the x_3-direction. At $x_2 = 1/3$ft, for example, the safe set extends to nearly 3.5ft in the x_3-direction (Fig. 4b, back plane). At $x_2 = 2.8$ft, the safe set extends to about 1.8ft in the x_3-direction (Fig. 4b, front plane). If x_2 starts small, then the flow rate into pond 2 will be small enough that the pond can release water fast enough to avoid overflowing, even if it starts full. However, as x_2 increases, the flow rate into pond 2 quickly surpasses the flow rate out of pond 2, so the pond must start at lower stages to avoid overflow.

Finally, consider Fig. 4c. The cross-section at any value of x_1 has a wedge-like boundary, where there is an inverse relationship between x_2 and x_3. For any initial value of x_1, as the stage of the stream starts higher, the stage of pond 2 must start lower to accommodate the increasing inflow rate from the stream. Further, as x_1 increases, the boundary of the (x_2, x_3)-cross-section erodes somewhat in the x_3-direction at higher stream stages. For example, at $x_1 = 0.6$ft, the safe set extends between 1.5-3.5ft in the x_3-direction for $x_2 \geq 1$ft (Fig. 4c, back wedge). At $x_1 = 4.8$ft, the safe set extends between 0.9-3.3ft in the x_3-direction for $x_2 \geq 1$ft (Fig. 4c, front wedge). As x_1 increases, the release rate of pond 1 increases modestly, which effectively transfers more water into pond 2. Thus, pond 2 must start at lower elevations to avoid overflow when the stream stage starts above about 1ft. These findings show that pond 1 moderately affects pond 2, although the ponds have similar release rates and their interactions are buffered by the dynamics of the stream.

E. Robustness Metrics

Previously, we explained how safe sets indicate the behavior of the stormwater system under various assumptions about surface runoff and valve positions. Now, we will discuss candidate metrics to quantify system robustness using a given safe set. A natural metric is the *percent volume* of the safe set with respect to the constraint set, since if the safe set has a larger volume, then there are more initial conditions from which the system operates satisfactorily. Another metric is the distance that the safe set extends along a *reference vector* that is chosen according to the relative importance of constraint satisfaction along each axis of the state space. In our case study, if it were equally critical that the ponds and the stream not overflow, then the reference vector would point approximately in the (5ft, 3ft, 3.5ft)-direction. A reference vector and the distance that the safe set of Sec. II-D.2 extends along this vector are provided for illustration (Fig. 5). Further, a system could be deemed sufficiently robust if a given *region* lies entirely inside the safe set.

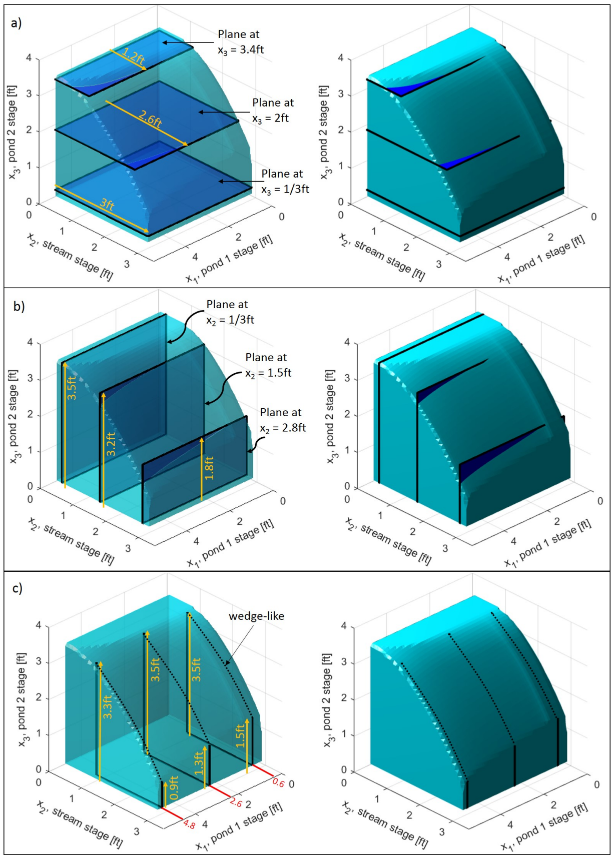

Fig. 4. The safe set at time zero, see (5), for the three-dimensional system with zero surface runoff and open valves over a four-hour time horizon ($T = 4$h). The equations of motion for the system are (1a)-(1c), such that $d_1 = d_2 = 0$ and $u_1 = u_2 = 1$ over time. Approximate two-dimensional cross-sections are shown along the (a) x_3-axis, (b) x_2-axis, and (c) x_1-axis. The boundary of the set is transparent on the left and opaque on the right.

The usefulness of a particular metric is system-dependent, and several metrics may be necessary to sufficiently quantify the robustness of a given system. The percent volume metric provides the proportion of states that are guaranteed to be safe and can be readily evaluated, but this metric does not specify how the safe states are distributed. Distance along the reference vector indicates whether the safe set is located in the more critical regions of the state space, but this metric may poorly describe the safe set as a whole and may be difficult to measure. The region metric can be readily evaluated, if a desired minimum level of robustness is known *a priori*. However, this metric provides a binary description of whether a certain level of robustness is feasible, which may not be sufficient to distinguish among multiple viable design options. As this work progresses, we expect the proposed robustness metrics to be refined and augmented with other summary descriptions of the safe set.

III. Outcome

Here we build on the three-dimensional example of Sec. II-D.2 to illustrate how safe sets and robustness metrics for quantifying these sets can be used to evaluate design options.

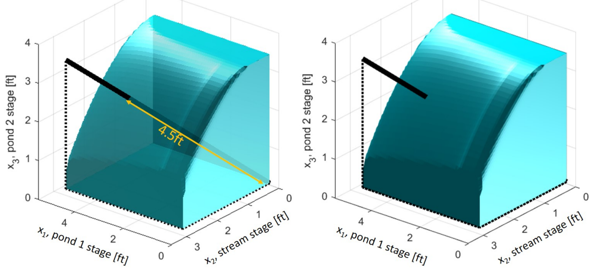

Fig. 5. A reference vector pointing approximately in the (5ft, 3ft, 3.5ft)-direction with the safe set of Sec. II-D.2. The distance that the safe set extends along the reference vector is approximately 4.5ft. The boundary of the set is transparent on the left and opaque on the right.

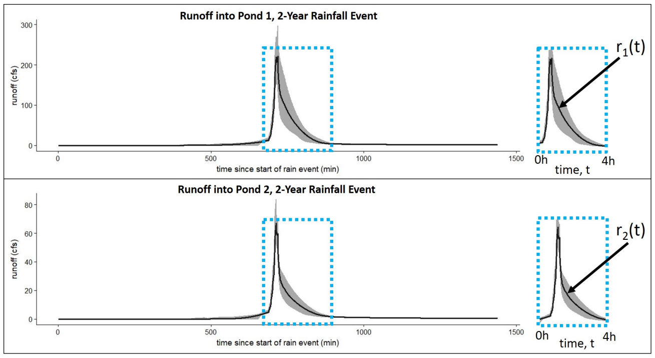

Fig. 6. Estimates of surface runoff into pond 1 (top) and pond 2 (bottom) from the two-year Type II 24-hour design storm for Lenexa, Kansas. A Monte Carlo approach was used to mitigate uncertainty in the estimated watershed parameters. 100,000 plausible runoff profiles of the same design storm were generated for each pond's watershed using PCSWMM (Computational Hydraulics International, Ontario), which extends USEPA's Storm Water Management Model (SWMM) [9]. The sample average is shown in black. 25 randomly chosen samples are shown in grey. The runoff estimates from PCSWMM are provided in minutely intervals. The functions, $r_1(t)$ and $r_2(t)$, were interpolated from the average runoffs into pond 1 and pond 2, respectively, during a four-hour segment of the storm. We used $r_1(t)$ and $r_2(t)$ to generate Fig. 7 (right column) and Fig. 8.

First, we provide safe sets at time zero for the three-dimensional system, given by (1a)-(1c), for four distinct design options and three distinct disturbance signals over a four-hour time horizon (Sec. III-A). Then, we study which design changes enable the system to attain a given level of robustness under a two-year design storm (Sec. III-B).

A. Preliminary Study

Initially, we examine four distinct design options in which the radius of the outlet of pond 2 is either R or $2R$, the surface area of pond 2 is either A_2 or $1.5A_2$, and the dynamic range of the outlets is either *passive* or *active* (Table I). *Passive* means that the outlets of both ponds are always open, as if real-time controls are not installed; $\mu(t) = [u_1, u_2]^T = [1, 1]^T$ for all $t \in [0, 4\text{h}]$. *Active* means that each outlet can vary continuously between open and closed over time; $\mu(t) = [u_1(t), u_2(t)]^T$, where $u_1(t)$ varies between 0 and 1, and $u_2(t)$ varies between 0 and 1, for all $t \in [0, 4\text{h}]$. The valve positions change based on an algorithm [2], [4] that monitors the current state and aims to prevent any element of the system from overflowing.[7] We consider two constant disturbance signals, $\gamma(t) = [d_1, d_2]^T = [0, 0]^T$ or $\gamma(t) = [d_1, d_2]^T = [2\text{cfs}, 2\text{cfs}]^T$ for all $t \in [0, 4\text{h}]$, and one time-varying disturbance signal, $\gamma(t) = [d_1(t), d_2(t)]^T = [r_1(t), r_2(t)]^T$. The functions, $r_1(t)$ and $r_2(t)$, are runoff estimates from a four-hour segment of a design storm (Fig. 6).

Our results illustrate how varying the system parameters impacts the resulting safe sets. Under zero runoff and small uniform runoff, the safe sets are large relative to the constraint set (4), which indicates that the system will not overflow starting from many initial conditions (Fig. 7, see left and center columns). However, under the two-year storm, the safe sets are empty (Fig. 7, see right column). This result suggests that, *if our modeling is sufficiently accurate*, then the ponds may not be adequately sized given the current characteristics of each watershed. Indeed, we may have undersized the ponds in the dynamic system model, or mischaracterized the watersheds in the rainfall-runoff model (PCSWMM), because neither our models nor their parameters have been formally validated. Further, it is possible that we are seeing the effects of recent urbanization and land use changes, since the ponds may have been designed when the region was substantially less developed.

B. Secondary Study

For the purpose of this paper, we ask if additional design options can accommodate the two-year storm (Fig. 6), assuming the current dynamic system model and runoff estimates. In particular, we study how the surface areas of the ponds and the types of outlet controls, *passive* or *active*, affect the size of the safe set at time zero. If the outlets are passive, then increasing the surface area of pond 1 by a factor of five and doubling the surface area of pond 2 yield a safe set that is empty (Fig. 8, Scenario M). However, if the outlets are active, these increases in surface area yield a safe set that is small, yet not empty, which suggests that active controls may improve the robustness of stormwater infrastructure (Fig. 8, Scenario N).

To further illustrate the use of reachability to inform design choices, we examine possible ways to satisfy a minimum level of robustness, as measured according to the distance of the safe set along a given reference vector. If the minimum level of robustness is 1ft, then $7A_1$ and $2.5A_2$ are sufficiently large surface areas of pond 1 and pond 2, respectively, under passive controls (Fig. 8, Scenario O). Now suppose that the required minimum level of robustness is 1.5ft. One option is to increase the surface areas of the ponds until this level of robustness is attained. However, there may be physical limits, such as steep terrain, or financial limits, such as high cost of land, which discourage us from examining the effect of further increases in pond surface area. Instead, we might consider evaluating the effect of active outlet controls, which yields a safe set that satisfies the new minimum robustness level (Fig. 8, Scenario P).

[7] The changes between valve positions are modeled as instantaneous switches.

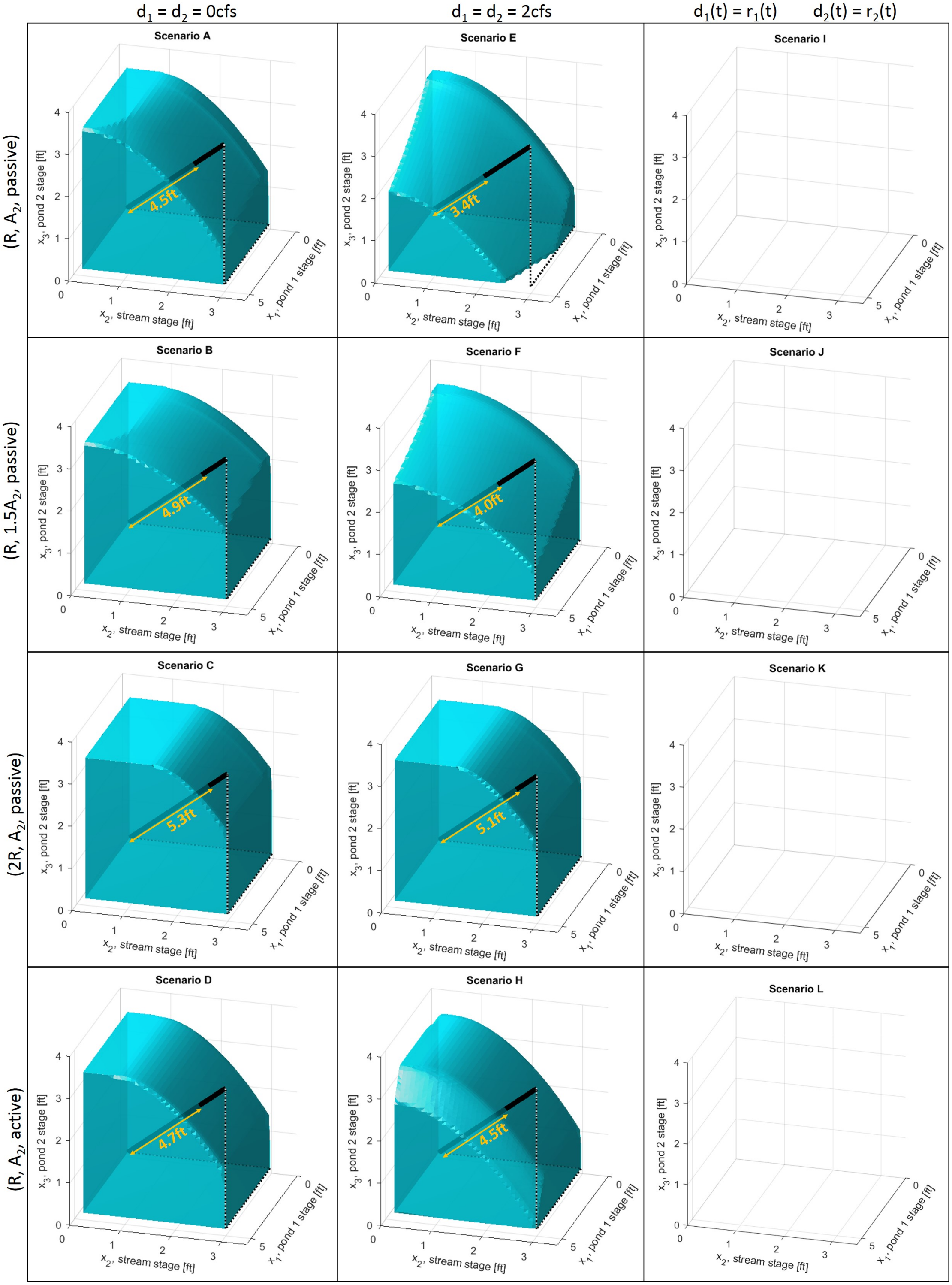

Fig. 7. Safe sets at time zero, see (5), for the three-dimensional system given by (1a)-(1c), for four distinct design options (rows) and three distinct disturbance signals (columns), over a four-hour time horizon ($T = 4$h). Each row is labeled with a tuple, (a, b, c), where a is the radius of the outlet of pond 2, b is the surface area of pond 2, and c is the dynamic range of both outlets. For example, in the top row, the radius of the outlet of pond 2 is $R = 8$in, the surface area of pond 2 is $A_2 = 259, 65\text{ft}^2$, and both outlets are *passive*. Each column corresponds to a particular disturbance signal. Left column: $\gamma(t) = [d_1, d_2]^T = [0, 0]^T$ for all $t \in [0, 4\text{h}]$. Center column: $\gamma(t) = [d_1, d_2]^T = [2\text{cfs}, 2\text{cfs}]^T$ for all $t \in [0, 4\text{h}]$. Right column: $\gamma(t) = [d_1(t), d_2(t)]^T = [r_1(t), r_2(t)]^T$, where $r_1(t)$ and $r_2(t)$ are based on a four-hour segment of a design storm (Fig. 6). The sets have a resolution of one inch along each axis. The sets in the right column are empty with respect to this resolution. A reference vector that points approximately in the (5ft, 3ft, 3.5ft)-direction is shown with each non-empty safe set. An estimate of the distance that each non-empty safe set extends along this vector is provided. Scenario A (row 1, column 1) is also shown in Fig. 4 and Fig. 5.

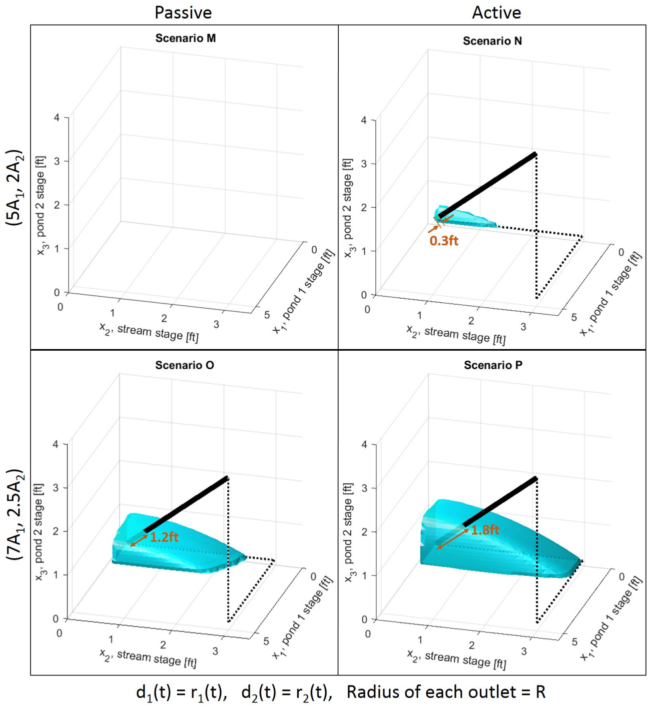

Fig. 8. Safe sets at time zero, see (5), for the three-dimensional system given by (1a)-(1c), such that $d_1(t) = r_1(t)$ and $d_2(t) = r_2(t)$ (see Fig. 6). Each row is labeled with (a, b), such that a is the surface area of pond 1, and b is the surface area of pond 2. The outlets of both ponds are *passive* (left column) or *active* (right column); see Sec. III-A for definitions of passive and active. A reference vector that points approximately in the (5ft, 3ft, 3.5ft)-direction is shown with each non-empty safe set. The sets have a resolution of one inch along each axis.

IV. Conclusion

In this paper, we demonstrated how reachability analysis can inform safety-critical design choices for stormwater infrastructure via a proof-of-concept case study. Reachability analysis augments existing stormwater design practices because it provides insight into system performance from a comprehensive set of physically realizable initial conditions, and insight into the consequences of interactions with nearby infrastructure, without requiring users to run individual simulations. We expect that, with further development and refinement, these methods will enhance the operational reliability of stormwater infrastructure.

Future work includes validation of the dynamic system model and the computational estimates of surface runoff. Further, it is necessary to design systems that are robust to uncertain timing and intensity in rainfall, and to develop robustness metrics that quantify the anticipated loss or damage associated with exceeding the constraints to a particular degree or for a particular duration. Toward these ends, we are developing a new framework for risk-sensitive reachability analysis. This framework will better quantify the realistic consequences of constraint violations, and encode surface runoff as a time-based sequence of random variables to provide probabilistic safety guarantees for rare events.

Acknowledgment

We thank Sylvia Herbert for assembling the reachability software for this paper and patiently explaining how to use it. We thank David Sedlak for advice and for connecting Claire Tomlin's group with OptiRTC, Inc. We thank Susmit Jha for discussions. We are grateful to the Computational Hydraulics International University Grant Program for the complementary use of PCSWMM Professional software for this project. M.C. is supported by the NSF Graduate Research Fellowship Program. K.S. is supported by an NSF Integrative Graduate Education and Research Training award (NSF 0966093). This work is supported in part by NSF CPS 1740079.

References

[1] "National pollutant discharge elimination system (NPDES)," https://www.epa.gov/npdes, Accessed: Sept. 1, 2017.

[2] I. M. Mitchell, A. M. Bayen, and C. J. Tomlin, "A time-dependent Hamilton-Jacobi formulation of reachable sets for continuous dynamic games," *IEEE Transactions on Automatic Control*, vol. 50, no. 7, pp. 947–957, Jul 2005.

[3] I. M. Mitchell and J. A. Templeton, "A toolbox of Hamilton-Jacobi solvers for analysis of nondeterministic continuous and hybrid systems," in *Hybrid Systems: Computation and Control*, M. Morari and L. Thiele, Eds. Berlin, Heidelberg: Springer, 2005, pp. 480–494. [Online]. Available: http://www.cs.ubc.ca/∼mitchell/ToolboxLS/

[4] S. Bansal, M. Chen, S. Herbert, and C. J. Tomlin, "Hamilton-Jacobi reachability: A brief overview and recent advances," *arXiv preprint arXiv:1709.07523*, 2017.

[5] D. M. Murray and S. J. Yakowitz, "Constrained differential dynamic programming and its application to multireservoir control," *Water Resources Research*, vol. 15, no. 5, pp. 1017–1027, Oct 1979.

[6] S. L. Herbert, M. Chen, S. Han, S. Bansal, J. F. Fisac, and C. J. Tomlin, "FaSTrack: A modular framework for fast and guaranteed safe motion planning," *arXiv preprint arXiv:1703.07373*, 2017.

[7] M. Chen, J. C. Shih, and C. J. Tomlin, "Multi-vehicle collision avoidance via Hamilton-Jacobi reachability and mixed integer programming," in *Decision and Control (CDC), 2016 IEEE 55th Conference on*. IEEE, Dec 2016, pp. 1695–1700.

[8] A. P. Davis and R. H. McCuen, *Stormwater Management for Smart Growth*. Springer Science & Business Media, 2005.

[9] L. A. Rossman, *Storm Water Management Model User's Manual, Version 5.0*. National Risk Management Research Laboratory, Office of Research and Development, US Environmental Protection Agency Cincinnati, 2010.

[10] I. M. Mitchell, "A toolbox of level set methods," UBC Department of Computer Science Technical Report TR-2007-11, Jun 2007.

[11] M. Chen, S. Herbert, and D. McPherson, "Hamilton-Jacobi optimal control toolbox (helperOC)," http://www.github.com/HJReachability/helperOC, Berkeley, CA, 2018.

[12] A. Akametalu, "A learning-based approach to safety for uncertain robotic systems," Ph.D. dissertation, EECS Department, University of California, Berkeley, May 2018. [Online]. Available: http://www2.eecs.berkeley.edu/Pubs/TechRpts/2018/EECS-2018-41.html