Risk-sensitive safety specifications for stochastic systems using Conditional Value-at-Risk*

Margaret P. Chapman, Jonathan P. Lacotte, Kevin M. Smith, Insoon Yang, Yuxi Han, Marco Pavone, Claire J. Tomlin

Abstract—This paper proposes a safety analysis method that facilitates a tunable balance between worst-case and risk-neutral perspectives. First, we define a risk-sensitive safe set to specify the degree of safety attained by a stochastic system. This set is defined as a sublevel set of the solution to an optimal control problem that is expressed using the Conditional Value-at-Risk (CVaR) measure. This problem does not satisfy Bellman’s Principle, thus our next contribution is to show how risk-sensitive safe sets can be under-approximated by the solution to a CVaR-Markov Decision Process. Our third and fourth contributions are to show that a value iteration algorithm solves the reduced problem and enables tractable policy synthesis for a class of linear systems. Fifth, we develop a realistic numerical example of a stormwater system to show that our approach can be applied to non-linear systems. Finally, we compare the CVaR criterion to the exponential disutility criterion. The latter allocates control effort evenly across the cost distribution to reduce variance, while the CVaR criterion focuses control effort on a given worst-case quantile—where it matters most for safety.

Index Terms—Conditional Value-at-Risk, Stochastic Optimal Control, Optimization, Linear Time-Varying Systems.

This paper was submitted for review in September 2019. This work was supported in part by the National Science Foundation (NSF) under Grant NSF PIRE UNIV59732, by the National Cancer Institute (NCI) Cancer Systems Biology Consortium “Measuring, Modeling and Controlling Heterogeneity” through Oregon Health and Science University NCI #1U54CA209988-01A1, and by the Computational Hydraulics International University Grant Program for complementary use of PCSSWMM Professional software. K. M. Smith was supported by an NSF Integrative Graduate Education and Research Training award (NSF 0966093). M. P. Chapman was supported by the NSF Graduate Research Fellowship Program.

M. P. Chapman and C. J. Tomlin are with the Department of Electrical Engineering and Computer Sciences, University of California Berkeley, Berkeley, CA 94720 USA (emails: chapmamm@berkeley.edu, tomlin@eecs.berkeley.edu).

J. P. Lacotte is with the Department of Electrical Engineering, Stanford University, Stanford, CA 94305 USA (email: lacotte@stanford.edu).

K. M. Smith is with the Department of Civil and Environmental Engineering, Tufts University, Medford, MA 02155 USA and OptiRTC, Inc., Boston, MA 02116 USA (email: kevin.smith@tufts.edu).

I. Yang is with the Department of Electrical and Computer Engineering, Seoul National University, Seoul, South Korea (email: insoonyang@snu.ac.kr).

Y. Han is with the Department of Mathematics, University of Wisconsin-Madison, Madison, WI 53706 USA (email: yuxi.han@wisc.edu).

M. Pavone is with the Department of Aeronautics and Astronautics, Stanford University, Stanford, CA 94305 USA (email: pavone@stanford.edu).

*An earlier version of this work was presented at the 2019 American Control Conference [23]. Unlike the earlier version, the current paper proves the correctness of the CVaR value iteration algorithm, proves the existence of optimal pre-commitment policies, provides a more general proof of the CVaR-MDP reduction method, develops a higher-dimensional stormwater system example, and illustrates the differences between CVaR and exponential disutility.

I. INTRODUCTION

CONTROL-theoretic formal verification methods for dynamic systems typically fall in the robust domain [1]–[5] or in the stochastic domain [6]–[9]. Robust methods for formal verification assume that uncertain disturbances lack probabilistic descriptions, live in bounded sets, and exhibit adversarial behavior. These assumptions are appropriate if probabilistic information about disturbances is not available, and if the conservative policy or safety specification that results from a pessimistic world view is useful in practice. However, when one considers formal verification as a design tool for safety-critical systems in the digital world today, it is reasonable to assume that simulation tools or sensor data are available to estimate probabilistic descriptions for disturbances. Moreover, it is reasonable to consider a more realistic world view: disturbances are not adversarial agents, but rare harmful outcomes are still possible in the long run.

Control-theoretic stochastic formal verification methods do assume that disturbances are probabilistic with non-adversarial [6] or adversarial [7]–[9] nature. These tools compute the probability of safety or performance using expected indicator cost functions. The expectation metric, however, does not address the possibility of distributions with large spread or the possibility of skewed distributions with “fat” harmful tails. Thus, there has been growing interest in the development of formal verification methods at the intersection of the robust and stochastic domains that specify robustness with respect to probability distributions [10] or utilize risk measure theory to quantify harmful tail costs [11], [23].

This recent work is closely related to the risk-sensitive optimal control paradigm pioneered by Peter Whittle [19]. Whittle showed that the expectation of an exponential disutility function is analogous to a mean-variance criterion, where the degree of disadvantage due to large variance can be tuned via a risk-sensitivity parameter [19]. The key assumption in this formulation is that the notion of risk in decision-making is sufficiently quantified through variance. In the case of asymmetric cost distributions skewed towards more harmful outcomes, however, quantifying risk in terms of variance may disregard realizations in the more harmful tail [20].

A strong theoretical basis for using the Conditional Value-at-Risk (CVaR) measure to explicitly address harmful tail costs has been developed since the early 2000s (e.g., see [21]). Intuitively, the Conditional Value-at-Risk of a continuous cost random variable is the expectation of the cost conditioned on the event that the cost takes on sufficiently large values. More precisely, as shown in Fig. 1, the Conditional Value-at-
Risk of a continuous cost random variable at level $\alpha$ is the expectation of the cost conditioned on the event that the cost exceeds its Value-at-Risk at level $\alpha$, which is the minimum cost in the $\alpha$ worst cases [22]. Conditional Value-at-Risk is a measure of the more harmful tail of a cost distribution, and managing this tail is paramount in safety-critical applications. (Outside the realm of formal verification, theoretical connections between robustness and risk measures, such as CVaR and exponential disutility, have been investigated [12], [13]. Concrete algorithms have been proposed to optimize policies for risk-sensitive Markov Decision Processes off-line [14], [15]. Scalable algorithms that use Q-learning techniques have been developed to extract approximate CVaR-optimal policies [16]. Also, a CVaR-constrained model predictive control (MPC) approach to risk-aware motion planning [17] and a risk-sensitive MPC framework for linear systems with stochastic multiplicative uncertainties [18] have been recently proposed.)

Statement of Contributions. First, we introduce the notion of a risk-sensitive safe set to specify the degree of safety of a stochastic dynamic system, which leverages the Conditional Value-at-Risk measure at a given risk-sensitivity level $\alpha$ [23]. Second, we show that risk-sensitive safe sets can be under-approximated by the solution to a Markov Decision Process (MDP), where the cost is assessed according to CVaR. This CVaR-MDP problem is time inconsistent, meaning that a policy that is optimal when viewed at time zero is not necessarily optimal when viewed at a later time, so dynamic programming cannot be directly applied (see discussion in [24]). However, a value iteration algorithm on the state space augmented by $Q$-learning techniques has been investigated [12], [13]. Con- stants for Conditional Value-at-Risk measure at a given risk-sensitivity level $\alpha$ [23]. Second, we show that risk-sensitive safe sets can be under-approximated by the solution to a Markov Decision Process (MDP), where the cost is assessed according to CVaR. This CVaR-MDP problem is time inconsistent, meaning that a policy that is optimal when viewed at time zero is not necessarily optimal when viewed at a later time, so dynamic programming cannot be directly applied (see discussion in [24]). However, a value iteration algorithm on the state space augmented by $Q$-learning techniques has been investigated [12], [13].

We use the following notation. If $X$ is any set and $f : X \rightarrow \mathbb{R}$ is bounded, then the uniform norm of $f$ is given by $\|f\|_u := \sup_{x \in X} |f(x)|$, where $|\cdot|$ is the Euclidean distance on $\mathbb{R}^n$. If $X$ is a metric space, then $B(X)$ is the Borel $\sigma$-algebra on $X$. If $A \in B(X)$, then $A$ is called a Borel set. If $1 \leq p \leq \infty$, then $L^p := L^p(\Omega, \mathcal{F}, \mathbb{P})$ is the collection of functions $f : \Omega \rightarrow \mathbb{R}$, measurable relative to $\mathcal{F}$ and $B(\mathbb{R})$, such that $\|f\|_p := \left(\int_{\Omega} |f|^p \mathbb{P} d\mathbb{P}\right)^{1/p} < \infty$ (i.e., random variables with finite $p^{th}$ moment, where $\mathcal{F}$ is a collection of events). $f \in L^\infty$ indicates that $f$ is a bounded random variable. If $f$ is a random variable defined on a probability space $(\Omega, \mathcal{F}, \mathbb{P})$, then $\sigma(f)$ is the $\sigma$-algebra generated by $f$, and $\mathbb{E}(f) := \int_{\Omega} f \mathbb{P} := \int_{\Omega} f(\omega) \mathbb{P}(d\omega)$ is the expected value of $f$. “Measurable” is short for Borel measurable, and “a.e.” stands for almost everywhere or almost every. “USC” denotes upper semi-continuous, and “LSC” denotes lower semi-continuous. Bold text signifies a determinstic quantity; e.g., $x_t = x$ indicates that the random variable $x_t$ takes on the value $x$.

There are various nearly equivalent definitions for Conditional Value-at-Risk (also called Average Value-at-Risk), and we use the following definition in this paper. Let $Y$ be a bounded random cost variable. The Conditional Value-at-Risk of $Y$ at risk-sensitivity level $\alpha \in [0,1]$ is defined as:

$$\text{CVaR}_\alpha(Y) := \begin{cases} \frac{1}{\alpha} \int_{\alpha}^{1} \text{VaR}_{1-\tau}(Y) d\tau & \text{if } 0 < \alpha \leq 1, \\ \|Y\|_\infty & \text{if } \alpha = 0, \end{cases}$$

(1a)

where

$$\text{VaR}_\alpha(Y) := \inf \left\{ y \in \mathbb{R} \mid \Pr \{ Y \leq y \} \geq 1 - \alpha \right\}$$

(1b)

is the Value-at-Risk at level $\alpha$, and $\|Y\|_\infty$ is the essential supremum (upper bound) of $Y$ [22, Thm. 6.2], [26]. One can show that $\text{CVaR}_0(Y) = \mathbb{E}(Y)$. If the cumulative distribution function of $Y$, $H_Y(y) := \Pr \{ Y \leq y \}$, is continuous at $y = \text{VaR}_\alpha(Y)$, then $\text{CVaR}_\alpha(Y) = \mathbb{E}(Y|Y \geq \text{VaR}_\alpha(Y))$, which is illustrated in Fig. 1, and which explains the name “Conditional Value-at-Risk” [22, Thm. 6.2].
For $\alpha \in [0, 1]$, CVaR$_{\alpha}$ is a coherent risk functional on the space of bounded random variables. This means that for fixed $\alpha \in [0, 1]$, CVaR$_{\alpha}$ : $L^\infty \to \mathbb{R}$ is convex, monotonic, translation equivariant (CVaR$_{\alpha}(Y + a) = CVaR_{\alpha}(Y) + a$ if $a \in \mathbb{R}$), and positively homogeneous (CVaR$_{\alpha}(\lambda Y) = \lambda CVaR_{\alpha}(Y)$ if $\lambda \geq 0$) [25], [26]. Moreover, since CVaR$_{\alpha}$ is a coherent risk functional, it is equivalent to an expectation maximized over a specific set of probability density functions [22, Thm. 6.4, Eqn. 6.40, Eqn. 6.70]. The above properties are mathematically useful and have intuitive interpretations. For example, the convexity of coherent risk functionals is consistent with the notion that the diversification of assets decreases risk. Moreover, CVaR$_{\alpha}$ may be considered a “robustified” expectation, since it is equivalent to a worst-case expectation with respect to certain perturbations in the assumed probability distribution [13].

III. PROBLEM FORMULATION

We use the Conditional Value-at-Risk measure to pose a safety specification problem for a given stochastic dynamic system over finite time. Suppose that the system dynamics take the form:

$$x_{t+1} = f_t(x_t, u_t, d_t), \quad t = 0, 1, \ldots, T - 1,$$

where $x_t \in X \subset \mathbb{R}^n$ is the state, $u_t \in U \subset \mathbb{R}^m$ is the control input, $d_t \in D \subset \mathbb{R}^q$ is the random disturbance, $f_t : X \times U \times D \to X$ is Borel measurable, and $X, U, D$ and $d$ are non-empty Borel sets. The disturbances $d_0, d_1, \ldots, d_{T-1}$ are random variables defined on a probability space $(\Omega, F, P)$, so each $d_i$ is a function from $\Omega$ to $D$ that is measurable relative to $F$ and $B(D)$. Assume that $d_0, d_1, \ldots, d_{T-1}$ are independent and identically distributed, where their common distribution is defined by the probability measure $P$ and is independent of all states and actions. Moreover, suppose that $P$ is a set of admissible control policies (to be specified precisely later), $K \subset X$ is a constraint set, and $g_K : \mathbb{R}^n \to \mathbb{R}$ is a bounded function that quantifies the extent of constraint violation (e.g., a clipped signed distance function from the boundary of $K$ [27, p. 8]). The risk-sensitive safe set in $(\alpha, r)$ is defined as:

$$S^r_{\alpha} := \{x \in X \mid W^r_{\alpha}(x, \alpha) \leq r\}, \quad (3a)$$

where

$$W^r_{\alpha}(x, \alpha) := \inf_{\pi \in \Pi_0} CVaR^\alpha_{\alpha}\left(\max_{t=0,1,\ldots,T} g_K(x_t) \mid x_0 = x\right), \quad (3b)$$

and the state trajectory $(x_0, x_1, \ldots, x_T)$ evolves under the policy $\pi \in \Pi_0$ according to (2) initialized at $x_0 = x$ [23].

The risk-sensitive safe set definition is well-motivated for several reasons. First, the definition incorporates different risk-sensitivity levels and non-binary distance to the constraint set, and thereby generalizes the classic maximal probabilistic safe set from [6]. Specifically, let $\epsilon \in [0, 1]$ be a maximum tolerable probability of constraint violation, and choose $\alpha = 1, r = \epsilon$, and $g_K(x) = 1_K(x)$, where $1_K(x) = 1$ if $x \notin K$ and $1_K(x) = 0$ if $x \in K$. Then, the risk-sensitive safe set at $(\alpha, r) = (1, \epsilon)$ is equal to:

$$\left\{x \in X \mid \inf_{\pi \in \Pi_0} \mathbb{E}\left[\max_{t=0,1,\ldots,T} 1_K(x_t) \mid x_0 = x\right] \leq \epsilon\right\}, \quad (4)$$

which is the maximal probabilistic safe set at the $\epsilon$-safety level [6] for a given stochastic system that evolves under policies in $\Pi_0$. Moreover, $S^r_{\alpha}$ encodes higher degrees of safety as $\alpha$ or $r$ decrease: $\alpha \geq 1_\alpha$ and $r_1 \geq r_2 \Rightarrow S^r_{\alpha_1} \subset S^r_{\alpha_2}$. Also, $S^r_{\alpha}$ specifies that the CVaR$_{\alpha}$ of the worst constraint violation of the state trajectory must be below a required threshold, whereas the safe set in [11] specifies that the CVaR$_{\alpha}$ of the constraint violation of $x_t$ must be below a required threshold for each $t$. So, $S^r_{\alpha}$ provides a risk-sensitive safety specification for the entire state trajectory. $S^r_{\alpha}$ is a well-motivated safety specification but difficult to compute due to the CVaR and the maximum in the definition of $W^r_{\alpha}$. To facilitate this computation, we use the following method.

Theorem 1 (Reduction to CVaR-MDP [23]): Fix $\beta > 0$ and $\gamma > 0$. For any $(\alpha, r) \in [0, 1] \times \mathbb{R}$, define the set $U^r_{\alpha} \subset X$ as follows:

$$U^r_{\alpha} := \{x \in X \mid J^r_{\alpha}(x, \alpha) \leq \beta e^{\gamma r}\}, \quad (5a)$$

where

$$J^r_{\alpha}(x, \alpha) := \inf_{\pi \in \Pi_0} CVaR^\alpha_{\alpha}\left(C_{0:T} \mid x_0 = x\right), \quad (5b)$$

such that the state trajectory evolves under the policy $\pi$ according to the dynamics model (2) initialized at $x_0 = x$, $c_t : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}$ is a stage cost, and $c_T : \mathbb{R}^n \to \mathbb{R}$ is a terminal cost. If $c_t = \beta e^{\gamma g_K}$ for all $t$, where $g_K : \mathbb{R}^n \to \mathbb{R}$ is bounded, then $U^r_{\alpha} \subset S^r_{\alpha}$. Moreover, the gap between $U^r_{\alpha}$ and $S^r_{\alpha}$ can be reduced by increasing $\gamma$.

Proof: Use the log-sum-exp relation in [31, Sec. 3.1.5] to show: for any $y \in \mathbb{R}^p$ and $\gamma > 0$,

$$\max_{i=1,2,\ldots,p} y_i \leq \frac{1}{\gamma} \log(\sum_{i=1}^p e^{\gamma y_i}) \leq \max_{i=1,2,\ldots,p} y_i + \log p / \gamma. \quad (6)$$

So, as $\gamma \to \infty, \frac{1}{\gamma} \log(\sum_{i=1}^p e^{\gamma y_i}) \to \max_{i=1,2,\ldots,p} y_i$.

Further, for any $\alpha \in [0, 1]$ and any bounded positive random variable $Z$, the following relation holds:

$$CVaR_{\alpha}(\log(Z)) \leq \log(CVaR_{\alpha}(Z)), \quad (7)$$

since $CVaR_{\alpha}(Z) = \sup_{t \in A} E_{E}(Z)$, where $A$ is a specific set of probability density functions by [22, Thm. 6.4, Eqn. 6.40, Eqn. 6.70], and since $E_{E}(\log(Z)) \leq \log(E_{E}(Z))$ for any $\xi \in A$ by Jensen’s Inequality. For any $\alpha \in [0, 1]$, $x \in X$, and $\pi \in \Pi_0$, the following inequalities hold:

$$CVaR_{\alpha}(\max_{t=0,1,\ldots,T} g_K(x_t) \mid x_0 = x) \leq \frac{1}{\gamma} CVaR_{\alpha}(\log(\sum_{t=0}^T e^{\gamma g_K(x_t)} \mid x_0 = x)), \quad (8)$$

by the relations cited above each inequality symbol, and since CVaR$_{\alpha}$ is monotonic and positively homogeneous. Take $x \in \mathcal{U}^r_{\alpha}$. For any $\epsilon > 0$, there exists $\pi_0 \in \Pi_0$ such that:

$$0 \leq CVaR_{\alpha}(\sum_{t=0}^T e^{\gamma g_K(x_t)} \mid x_0 = x) \leq \epsilon + \inf_{\pi_0 \in \Pi_0} CVaR_{\alpha}(\sum_{t=0}^T e^{\gamma g_K(x_t)} \mid x_0 = x) \leq \epsilon + e^{\gamma r}, \quad (i)$$

for the following reasons: (i) $\forall y \in X, e^{\gamma g_K(y)} > 0$, (ii) definition of supremum and $g_K$ is bounded, (iii) $x \in \mathcal{U}^r_{\alpha}$.

\footnote{Abate et al. [6] used the formalism of stochastic hybrid systems, which we do not utilize in the current paper.}
CVar$^2_\gamma$ is positively homogeneous, and $\beta > 0$. Take the logarithm of both sides and divide by $\gamma > 0$ to obtain:

$$\frac{1}{\gamma} \log \left( \text{CVar}^\gamma_{\alpha} \left( \sum_{t=0}^{T} e^{\gamma g_k(x_t)} \big| x_0 = x \right) \right) \leq \frac{1}{\gamma} \log (\epsilon + e^{\gamma \tau}) . \tag{9}$$

Use the definition of $W^*_0$ (3b) as an infimum to find:

$$W^*_0 (x, \alpha) \leq \text{CVar}^\gamma_{\alpha} \left( \max_{t=0, \ldots, T} g_k(x_t) \big| x_0 = x \right) \leq \frac{1}{\gamma} \log (\epsilon + e^{\gamma \tau}) . \tag{8}$$

$$W^*_0 (x, \alpha) \leq \frac{1}{\gamma} \log (\text{CVar}^\gamma_{\alpha} \left( \sum_{t=0}^{T} e^{\gamma g_k(x_t)} \big| x_0 = x \right) \leq \frac{1}{\gamma} \log (\epsilon + e^{\gamma \tau}) ,$$

where the appropriate relation is cited above each inequality symbol. Finally, since $W^*_0 (x, \alpha) \leq \frac{1}{\gamma} \log (\epsilon + e^{\gamma \tau})$ for any $\epsilon > 0$, take $\epsilon \rightarrow 0$ and apply continuity of the logarithm to obtain $W^*_0 (x, \alpha) \leq r$. So, $x \in S^\alpha_\gamma$.

**Remark 1:** In Theorem 1, the parameter $\beta$ is included to counter numerical issues that arise when $\gamma$ is large.

Theorem 1 indicates that $U^*_\alpha$ is an under-approximation of the risk-sensitive safe set $S^\alpha_\gamma$. The purpose of Theorem 1 is to approximate the maximum in the definition of $S^\alpha_\gamma$ in terms of a summation, since the latter is more amenable to computation due to translation equivariance (CVar$^\gamma_\alpha (Y + a) = \text{CVar}^\gamma_{\alpha} (Y) + a$ if $a \in \mathbb{R}$). However, computing the function $J^*_\alpha$, as defined in Theorem 1, is still difficult because the Conditional Value-at-Risk measure is *time inconsistent* [28].

Intuitively, time inconsistency implies that a policy that is optimal when viewed at time zero is not necessarily optimal when viewed at a later time [24]. Thus, a standard dynamic programming value iteration algorithm, such as [30, Sec. 1.3], cannot be used to compute $J^*_\alpha$. In the next section, taking inspiration from [13], [25], and [23], we prove that a value iteration algorithm on the augmented state space $X := X \times [0, 1]$ correctly computes $J^*_\alpha$, by imposing additional structure on the problem.

**IV. CVAR Value Iteration Algorithm**

We consider a value iteration algorithm on $X := X \times [0, 1]$ that induces dynamics on the risk-sensitivity level. The algorithm involves optimizing over a set of probability densities (i.e., weights) to determine the risk-sensitivity level at a given time, so a desired risk-sensitivity level is attained over the entire horizon. We specify this set of probability densities next and use $\alpha_t$ to denote the risk-sensitivity level at time $t$.

**Definition 1 (Risk Envelope):** Fix $t$, $x_t = x \in X$, $u_t = u \in U$, and $\alpha_t = \alpha \in [0, 1]$. The risk envelope for time $t$ is defined as follows:

$$R^\alpha_t (x, u) := \left\{ Z : \Omega \rightarrow \mathbb{R} \bigg| \begin{array}{l}
\sigma (f_t (x, u, d_t)) - \text{-measurable}, \\
\int_{\Omega} Z d\mathbb{P} = 1, \\
0 \leq \alpha Z (\omega) \leq 1 \text{ for a.e. } \omega \in \Omega
\end{array} \right\} . \tag{10}$$

where $\int_{\Omega} Z d\mathbb{P} := \int_{\Omega} Z (\omega) d\mathbb{P} (d\omega)$ is the expectation of $Z$ with respect to the probability measure $\mathbb{P}$, $(\Omega, \mathcal{F}, \mathbb{P})$ is the probability space upon which the random disturbance $d_t$ is defined, and $\sigma (f_t (x, u, d_t))$ is a sub-$\sigma$-algebra of $\mathcal{F}$.

The following algorithm, originally proposed by [13], defines the value function at time $t$ in terms of a stage cost $c_t$ and a worst-case weighted expected value function at time $t + 1$. Here, the meaning of worst-case is specified by optimizing over the risk envelope for time $t$.

**Algorithm 1 (CVAR Value Iteration):** Define the functions $J_{t-1}, \ldots, J_1, J_0$ recursively as follows: $\forall (x, \alpha) \in X$ and $t = T - 1, \ldots, 0$,

$$J_t (x, \alpha) := \inf_{u \in U} \left\{ c_t (x, u) + \right. \sup_{Z \in R^\alpha_t \mid x, u} \left( \int Z (\omega) \cdot J_{t+1} (f_t (x, u, d_t (\omega)), \alpha Z (\omega)) d\mathbb{P} (d\omega) \right) \right\} , \tag{11}$$

with the terminal condition $J_T (x, \alpha) := c_T (x)$.

In this section, we will prove that $J^*_\alpha$, as defined by (5b), is equivalent to $J_0$, as defined by Algorithm 1, by specifying additional structure on the problem, including linear time-varying (LTV) dynamics and history-dependent policies.

**Assumption 1 (Conditions on Control System):** The following conditions hold:

1) $x_{t+1} = f_t (x_t, u_t, d_t) := A_t x_t + B_t u_t + E_t d_t$ for $t = 0, \ldots, T - 1$. The matrices $A_t \in \mathbb{R}^{n \times n}$, $B_t \in \mathbb{R}^{n \times m}$, and $E_t \in \mathbb{R}^{n \times q}$ are given for each $t$. The initial condition $x_0 = x$ is deterministic.

2) The stage cost functions $c_t : \mathbb{R}^n \times \mathbb{R}^m \rightarrow \mathbb{R}$ for $t = 0, 1, \ldots, T - 1$ and the terminal cost function $c_T : \mathbb{R}^n \rightarrow \mathbb{R}$ are bounded, convex, and continuous.

3) The action space $U \subset \mathbb{R}^m$ is non-empty, compact, and convex.

Many practical control systems can be modeled by linear time-varying dynamics with compact, convex action spaces and convex, continuous stage (or terminal) costs. A concrete example can be found in Section VII-B. Moreover, Assumption 1 ensures that a minimax equality holds, and this minimax equality (which was not shown by [13]) is required to prove the validity of Algorithm 1. In the following definition, we specify the set of admissible control policies as being non-anticipatory, deterministic, and history-dependent.

**Definition 2 (Set of Admissible Policies):** The set of admissible policies for time $t = 0, 1, \ldots, T - 1$ is defined as follows:

$$\Pi_t := \left\{ \pi_t := (\mu_t, \mu_{t+1}, \ldots, \mu_{T-1}) \bigg| \begin{array}{l}
\text{each } \mu_k : H_{t:k} \rightarrow U \\
\text{is Borel measurable}
\end{array} \right\} , \tag{12}$$

where $H_{t:k} := (X \times \mathbb{R})^{k-t} \times X$ is the set of histories from time $t$ to time $k$, whose elements take the form $h_{t:k} := (x_t, u_t, \ldots, x_{k-1}, u_{k-1}, x_k)$.

**Remark 2:** We specify history-dependent policies above instead of standard Markov policies. This is necessary because the CVaR criterion (5b) does not satisfy certain critical properties that hold for standard expected cost functions, including: time consistency [28], [29], the principle of optimality [30, Sec. 1.3], and the tower rule [32, Prop. B.1 (c)].

The next definition specifies the CVaR-optimal cost-to-go at time $t$ in terms of the set of history-dependent policies $\Pi_t$.

**Definition 3 (CVaR-Optimal Cost-to-Go):** The CVaR-optimal cost-to-go function $J^*_t : X \rightarrow \mathbb{R}$ at $t = 0, 1, \ldots, T - 1$ is defined as follows:

$$J^*_t (x, \alpha) := \inf_{\pi_t \in \Pi_t} \text{CVar}^\gamma_{\alpha} (C_{t:T} | x_t = x) , \tag{13a}$$
where \( C_{t,T} \) is the random cumulative cost of the state trajectory for time \( t \),
\[
C_{t,T} := c_T(x_t) + \sum_{k=t}^{T-1} c_k(x_k, \mu_k(h_{t:k})),
\]
(13b)
such that the state trajectory evolves under \( \pi_t := (\mu_t, \mu_{t+1}, \ldots, \mu_{T-1}) \in \Pi_t \) via the LTV dynamics initialized at \( x_t = x \). Moreover, we define the optimal terminal cost \( J_T^\pi(x_t, \alpha) := c_T(x_t) \) for all \( \alpha \in [0, 1] \).

Since we have specified Assumption 1, the set of history-dependent policies \( \Pi_t \), and the CVaR-optimal cost-to-go function \( J_t^* \), we are ready to state the main result of this section.

**Theorem 2 (Validity of CVaR Value Iteration):** The value function \( J_t \), as defined recursively by Algorithm 1, is equivalent to the CVaR-optimal cost-to-go function \( J_t^* \), as defined by (13a), for \( t = 0, 1, \ldots, T \).

Theorem 2 is significant because it allows us to compute the risk-sensitive safe set under-approximation \( \mathcal{R}_t^\alpha(x, u) \) and \( \mathcal{R}_T^\alpha(x, u) \), using these two lemmas to prove Theorem 2.

**Proof:** We use Sion’s Minimax Theorem [34, Thm. 1.1]. \( \mathcal{R}_t^\alpha(x, u) \) is a non-empty, convex, and compact set in \( L^2 := \mathbb{L}^2(\mathcal{F}_t, \mathbb{P}) \) with the weak topology by Lemma 5. \( H(\cdot, \pi) \) is concave on \( \mathcal{R}_t^\alpha(x, u) \) for any \( \pi \in \Pi_t+1 \), by [25, Thm. 12] applied to a random cost, and by linearity of expectation. For any \( \pi \in \Pi_t+1 \), \( H(\cdot, \pi) \) is upper semi-continuous in the relative weak topology on \( \mathcal{R}_t^\alpha(x, u) \) in \( L^2 \) by [35, Prop. 2.10, p. 72], since \( H(\cdot, \pi) \) is real-valued, concave, and upper semi-continuous in the relative norm topology on \( \mathcal{R}_t^\alpha(x, u) \subset L^2 \) (Lemma 4, Lipschitz \( \implies \) upper semi-continuous). Moreover, since \( \mathcal{R}_t^\alpha(x, u) \subset L^2 \), we have \( \mathcal{R}_t^\alpha(x, u) \subset L^2 \) by Lemma 4, Lipschitz \( \implies \) upper semi-continuous. Hence, we are ready to prove Theorem 2. In particular, we show that the value function \( J_t \), as defined recursively by Algorithm 1, is equivalent to the CVaR-optimal cost-to-go function \( J_t^* \), as defined by (13a), for each \( t \). This equivalence means that we can compute the risk-sensitive safe set under-approximation \( \mathcal{U}_t^\alpha \), as defined by (5), using Algorithm 1. Next, we prove Theorem 2 by induction.

**Proof:** \( J_t^* = J_t \) by definition. Assume \( J_t^* = J_t^* \) for
some $t$. Take $(x, \alpha) \in X$. Then, $J_t^*(x, \alpha)$ equals the following:

\[
J_t^*(x, \alpha) = \inf_{u \in U} \left\{ c_t(x, u) + \inf_{\pi \in \Pi_t} \text{CVaR}_\alpha(\pi \circ \gamma_{t+1}^{i+1}(x_t = x, u_t = u)) \right\}
\]

\[
= \inf_{u \in U} \left\{ c_t(x, u) + \inf_{\pi \in \Pi_t} \sup_{Z \in \mathbb{R}_+^1(x, \pi, u)} H_t^\alpha(Z, \pi, u) \right\}
\]

\[
= \inf_{u \in U} \left\{ c_t(x, u) + \sup_{Z \in \mathbb{R}_+^1(x, \pi, u) \in \Pi_t} H_t^\alpha(Z, \pi, u) \right\},
\]

where

\[
H_t^\alpha(Z, \pi, u) := \int \mathbb{P}(\omega) \cdot \text{CVaR}_\alpha(Z(\omega) \circ \gamma_{t+1}^{i+1}(x_t = x, u_t = u)),
\]

such that $\gamma_{t+1}^{i+1}$ is conditioned on $x_{t+1} = f_t(x, u, d_t(\omega)) := A_t x + B_t u + E_t d_t(\omega)$ in the integral above, and $(\Omega, \mathcal{F}, \mathbb{P})$ is the probability space upon which the random disturbance $d_t$ is defined. We justify each equality: (i) equivalence between minimization over $u_t : H_{t+1} \to U$ and $u \in U$ when $x_t = x$ is given, and CVaR is translation equivariant; (ii) Lemma 1; and (iii) Lemma 2. Moreover, the following equalities hold:

\[
\inf_{\pi \in \Pi_t} H_t^\alpha(Z, \pi, x, u) = \int \mathbb{P}(\omega) \cdot \text{CVaR}_\alpha(Z(\omega) \circ \gamma_{t+1}^{i+1}(x_t = x, u_t = u))
\]

\[
= \int \mathbb{P}(\omega) \cdot J_{t+1}(f_t(x, u, d_t(\omega)), \alpha Z(\omega))
\]

\[
\int \mathbb{P}(\omega) \cdot J_{t+1}(f_t(x, u, d_t(\omega)), \alpha Z(\omega))
\]

where we justify each step: (iv) interchangeability assertion from the proof of [25, Thm. 18, p. 162]; (v) definition of $J_t^*$ (13a), and $\gamma_{t+1}^{i+1}$ is conditioned on $x_{t+1} = f_t(x, u, d_t(\omega))$ in the previous line; and (vi) induction hypothesis $J_{t+1}^* = J_{t+1}$. The above steps together with (11) show that $J_t^* = J_t$, which completes the induction.

We have shown that $J_t^*$, as defined by (13a), is equal to $J_t$, as defined by Algorithm 1, for $t = 0, 1, \ldots, T - 1$, under the conditions specified in Assumption 1. In the next section, we prove the existence of tractable policies that attain $J_t^*$, if we pre-commit to the dynamics of the risk-sensitivity level induced by Algorithm 1.

V. SYNTHESIS OF PRE-COMMITMENT POLICIES

Our approach to the synthesis of optimal policies involves restricting the optimization space of history-dependent policies to policies that commit to specific risk-sensitivity level dynamics. Such policies are called pre-commitment policies. This restriction to pre-commitment policies is well-motivated for two reasons. First, due to time inconsistency, a Conditional Value-at-Risk cost function is not amenable to dynamic programming unless the entire history is recorded [25]. Second, computing history-dependent policies is intractable generally, since substantial memory and computation time are required. However, we can overcome these two challenges by restricting the optimization space to policies that commit to risk-sensitivity level dynamics that summarize the history.

The purpose of this section is to synthesize tractable policies that attain the CVaR-optimal cost-to-go function $J_t^*$ (13a) under mild restrictions on the optimization space of history-dependent policies $\Pi_t$. We define a control law at time $k \geq t$ on the augmented state space $X := X \times [0, 1]$ that is a function of the current state $x_k$ and the current risk-sensitivity level $\alpha_k$. Accordingly, this law is called an $X$-Markov control law. The current state $x_k \in X$ satisfies the linear time-varying dynamics specified by Assumption 1. The current risk-sensitivity level $\alpha_k \in [0, 1]$ satisfies particular dynamics induced by Algorithm 1. Under these dynamics, $\alpha_k$ is a one-dimensional parameter that summarizes the higher-dimensional prior history $(x_1, u_1, x_1, u_1, \ldots, x_k, u_k) \in (X \times U)^k$.

This section is structured as follows. First, we specify a regularity condition on the risk envelope to facilitate policy synthesis (Assumption 2). Second, we define $X$-Markov control laws and $X$-Markov policies (Definition 4). We prove the existence of $X$-Markov control laws by invoking Assumptions 1 and 2. Third, we define the dynamics of the risk-sensitivity level induced by Algorithm 1 (Definition 5). Finally, in Theorem 3, we show that $X$-Markov policies attain the CVaR-optimal cost-to-go function (13a), if we pre-commit to the risk-sensitivity level dynamics induced by Algorithm 1.

A. Regularity Condition on Risk Envelope

Here, we specify and justify a regularity condition on the risk envelope defined by (10).

Assumption 2 (Regularity Condition on Risk Envelope): The set-valued mapping $(x, \alpha, u) \mapsto R_c^u(x, \alpha, u)$ is lower semi-continuous on $X \times U$.

Assumption 2 is useful in general, since it guarantees the existence of policies that optimize certain performance criteria. For example, in the classic setting of games against nature, where stochastic control systems are affected by adversarial players with unknown distributions, the set of admissible actions of the adversary (player 2) is assumed to be lower semi-continuous in the state and action of the controller (player 1) [38, Assumption 3.1 (g), p. 1632]. Also, Assumption 2 resembles conditions in the risk-averse dynamic programming literature. Ruszczyński [37] assumes that the stochastic transition kernel is continuous in the control and the risk envelope is lower semi-continuous in the probability measure, implying that the risk envelope is lower semi-continuous in the control by composition [37, Thm. 2 (i) (iii)]. The conditions in [37] are required for a time-consistent problem, whereas the condition in Assumption 2 is required for a time-inconsistent problem.

Assumption 2 is a measurable selection condition for time-inconsistent CVaR-MDP problems that guarantees the existence of a $X$-Markov control law. In the next subsection, we define a $X$-Markov control law in terms of an argument that minimizes an objective function over a compact set. To ensure that a minimum argument exists, the objective function must be lower semi-continuous. Assumption 2 specifies a sufficient condition to guarantee that the objective function is indeed lower semi-continuous.

The condition specified in Assumption 2 is equivalent to the following statement. If $(x_n, \alpha_n, u_n) \to (x, \alpha, u)$ in $X \times U$ and $Z \in R_c^u(x, \alpha, u)$, then there exist $Z_n \in R_c^u(x_n, \alpha_n, u_n)$ s.t. $Z_n \to Z$ [32, Prop. D.2, p. 182].

Measureable selection conditions for standard MDPs, where expected costs are assessed, can be found in [32, Sec. 3.3].
B. Existence of $X$-Markov Policies

Recall that $X := X \times [0, 1]$ is the state space augmented by the space of risk-sensitivity levels. Here, we define $X$-Markov control laws as Borel measurable mappings from $X$ to $U$ and $X$-Markov policies as time-based sequences of such mappings. Then, we prove the existence of $X$-Markov control laws using the conditions specified in Assumptions 1 and 2.

**Definition 4 ($X$-Markov Control Law, Policy):** Fix $t$. A $X$-Markov control law at time $t$ is a Borel measurable function $\mu^*_t : X \rightarrow U$ that satisfies the following: $\forall (x, \alpha) \in X$,

$$
\mu^*_t(x, \alpha) \in \arg\min_{u \in U} \left\{ c_t(x, u) + \sup_{Z \in \mathbb{R}^+_t(x, u)} G^0_t(Z, x, u) \right\},
$$

such that $(x_t, \alpha_t) = (x, \alpha)$ is the state and risk-sensitivity level at time $t$, and $G^0_t(Z, x, u)$ is defined as:

$$
G^0_t(Z, x, u) := \int_{\Omega} Z(\omega) \cdot J_{t+1} \left( f_t(x, u, \alpha_t) \right) \cdot \alpha Z(\omega) \mathbb{P}(d\omega),
$$

where $f_t(x, u, \alpha_t) := A_x x + B_x u + E_t \mathbb{E}(d_t(\omega), x_t = x)$ is the state at time $t$, $u_t = u$ is the control at time $t$, and $(\Omega, \mathcal{F}, \mathbb{P})$ is the probability space upon which the random disturbance $d_t$ is defined. A sequence of $X$-Markov control laws $\pi^*_t := (\mu^*_t, \mu^*_t, \ldots, \mu^*_{t-1})$ is a $X$-Markov policy for time $t$.

The arguments in Lemmas 3, 6, and 7 together show the existence of $X$-Markov control laws, by invoking Assumptions 1 and 2. Lemma 3 specifies that the objective function in (18) is lower semi-continuous in $u$ to ensure the existence of a $X$-Markov control law, if $G^0_t(Z, x, u)$ is lower semi-continuous in $(Z, u)$. Lemma 6 specifies that $G^0_t(Z, x, u)$ is lower semi-continuous in $(Z, u)$, if $J^{t+1}_t$ is lower semi-continuous (Appendix II). Finally, Lemma 7 specifies that $J^{t+1}_t$ is lower semi-continuous for each $t$ (Appendix II). We provide the statements and proofs of Lemmas 6 and 7 in Appendix II, while we provide the statement and proof of Lemma 3 next.

**Lemma 3 (Existence of $X$-Markov Control Laws):** Fix $t$, and define $v_t : X \times U \rightarrow \mathbb{R}$ as follows:

$$
v_t(x, \alpha, u) := c_t(x, u) + \sup_{Z \in \mathbb{R}^+_t(x, u)} G^0_t(Z, x, u),
$$

where $\mathbb{R}^+_t(x, u)$ is given by (10), and $G^0_t(Z, x, u)$ is given by (19). Then, there exists a Borel measurable function $\mu^*_t : X \rightarrow U$ that satisfies the following statement: $\forall (x, \alpha) \in X$,

$$
v_t(x, \alpha, \mu^*_t(x, \alpha)) = \inf_{u \in U} v_t(x, \alpha, u) = \min_{u \in U} v_t(x, \alpha, u).
$$

**Proof:** Since $U$ is compact, it suffices to show that $v_t(x, \alpha, \cdot)$ is lower semi-continuous on $U$ for every $(x, \alpha) \in X$ by [32, Prop. D.5 (a)]. Since the sum of lower semi-continuous functions is lower semi-continuous, it suffices to show that $u \mapsto \psi^*_t(x, \alpha)$ is lower semi-continuous on $U$ for every $(x, \alpha) \in X$. Since $u \mapsto \mathbb{R}^+_t(x, u)$ is a lower semi-continuous set-valued mapping by Assumption 2, for any $\{u^{(j)}\} \subset U$ converging to a point $u \in U$ and for any $Z \in \mathbb{R}^+_t(x, u)$, there exists $Z^{(j)} \in \mathbb{R}^+_t(x, u^{(j)})$ such that $Z^{(j)} \rightarrow Z$. If $G^0_t(Z, x, u)$ is lower semi-continuous in $(Z, u)$, then one can show:

$$
\lim_{j \rightarrow \infty} \psi^*_t(x, \alpha) \geq \lim_{j \rightarrow \infty} G^0_t(Z^{(j)}, x, u^{(j)}) \geq G^0_t(Z, x, u),
$$

by the definition of supremum and lower semi-continuity, respectively. Since the above inequalities hold for any $Z \in \mathbb{R}^+_t(x, u)$, and since the supremum is the least upper bound,

$$
\liminf_{j \rightarrow \infty} \psi^*_t(x, \alpha) \geq \sup_{Z \in \mathbb{R}^+_t(x, u)} G^0_t(Z, x, u) =: \psi^*_t(x, \alpha),
$$

showing that $\psi^*_t(x, \alpha)$ is lower semi-continuous on $U$, the desired result. (See [38, Lemma 3.2 (a)] for the original proof.) So, it suffices to show that $G^0_t(Z, x, u)$ is lower semi-continuous in $(Z, u)$, which is shown in Lemma 6 (Appendix II).

Next, we specify the dynamics of the risk-sensitivity level so that $X$-Markov policies under these dynamics are history-dependent.

C. Risk-Sensitivity Level Dynamics

Here, we define the risk-sensitivity level dynamics in terms of a member of the risk envelope that maximizes a weighted CVaR-optimal cost-to-go in expectation.

**Definition 5 (Risk-Sensitivity Level Dynamics):** Fix $t$, $x_t = x \in X$, $u_t = u \in U$, and $\alpha_t = \alpha \in [0, 1]$. Let $Z^*_t \in \mathbb{R}^+_t(x, u)$ satisfy the following statement:

$$
Z^*_t \in \arg\max_{Z \in \mathbb{R}^+_t(x, u)} G^0_t(Z, x, u),
$$

where $G^0_t(Z, x, u)$ is defined by (19). Then, the risk-sensitivity level at time $t + 1$ is given by $\alpha_{t+1} = \alpha \cdot Z^*_t$.

Please note the following remarks concerning the risk-sensitivity level dynamics defined above.

**Remark 3:** Lemma 5 and Lemma 8 ensure that $Z^*_t \in \mathbb{R}^+_t(x, u)$ is well-defined, since the supremum of an upper semi-continuous map on a compact topological space is attained [33, Thm. A6.3]. Lemma 5 specifies that the risk envelope $R^\alpha_t(x, u)$ is compact in $L^2 := L^2(\Omega, \sigma(f_t(x, u, d_t)), \mathbb{P})$ endowed with the weak topology (Appendix I). Lemma 8 specifies that $G^0_t(\cdot, x, u)$ is upper semi-continuous in the relative weak topology on $\mathbb{R}^+_t(x, u) \subset L^2$ (Appendix II).

**Remark 4:** The risk-sensitivity level at time $t + 1$, $\alpha_{t+1} = \alpha \cdot Z^*_t$, is a $\sigma(f_t(x, u, d_t))$-measurable random variable, since $Z^*_t$ is. If $\omega \in \Omega$ is fixed (which implies that $d_t(\omega)$ occurs at time $t$), then the risk-sensitivity level that occurs at time $t + 1$ is given by $\alpha_{t+1}(\omega) = \alpha \cdot Z^*_t(\omega)$.

**Remark 5:** $X$-Markov policies (Definition 4) under the dynamics of the risk-sensitivity level (Definition 5) are history-dependent policies. Specifically, a $X$-Markov policy for time $t$ is a function of the augmented state trajectory $(x_t, \alpha_t, x_{t+1}, \alpha_{t+1}, \ldots, x_T, \alpha_T)$ by Definition 4, where $\alpha_k$ is a function of $(\alpha_t, x_t, u_t, \ldots, x_{k-1}, u_{k-1})$ for $k = t + 1, t + 2, \ldots, T$ by Definition 5 and [33, Thm. 6.4.2 (c), p. 251].

D. Optimality of Pre-Commitment $X$-Markov Policies

The CVaR-optimal cost-to-go $J^*_t$ (13a) is an infimum over a set of history-dependent policies $\Pi_t$ (Definition 2). The final theorem of this paper indicates that $X$-Markov policies (Definition 4) attain $J^*_t$, if we pre-commit to the risk-sensitivity level dynamics given by Definition 5. This is a powerful practical result because history-dependent policies are generally intractable due to extensive memory requirements, but the following theorem enables tractable computations.

**Theorem 3 (Optimal Pre-Commitment Policies):** Fix $t$. Let $\pi^*_t := (\mu^*_t, \mu^*_{t+1}, \ldots, \mu^*_{T-1})$ be a $X$-Markov policy for time
where $t$, where the risk-sensitivity level dynamics are given by Definition 5. Then, $\pi^*_t \in \Pi_t$ is an optimal pre-commitment policy, i.e., the following equality holds: $\forall (x, \alpha) \in \mathbb{X}$,

$$J^*_t(x, \alpha) = \text{CVA}\text{R}^*_\alpha (C_{t:T}|x_t = x),$$

(22)

where

$$\begin{align*}
C_{t:T} &= c_T(x_T) + \sum_{k=t}^{T-1} c_k(x_k, \mu^*_k(x_k, \alpha_k)),
\end{align*}$$

and $(x_t, \alpha_t, \ldots, x_T, \alpha_T)$ satisfies the linear time-varying dynamics (Assumption 1) and the risk-sensitivity level dynamics (Definition 5) under $\pi^*_t$ initialized at $(x_t, \alpha_t) = (x, \alpha)$.

**Proof:** We proceed by induction. Since $J^*_T(x_T, \alpha_T) = c_T(x_T)$ does not depend on the control when $(x_T, \alpha_T) = (x, \alpha)$ is given, the base case is $t = T - 1$. In this case, $\pi^*_{t-1} = \mu^*_{t-1}$, where $u_{t-1} = \mu^*_{t-1}(x, \alpha)$. Then, the following equalities hold:

$$\text{CVA}\text{R}^*_\alpha (C_{t:T-1}|x_{t-1} = x) = \text{CVA}\text{R}^*_\alpha (c_T(x_T)|x_{t-1} = x, u_{t-1} = \mu^*_{t-1}(x, \alpha))$$

(23)

where $(x_t, \alpha_t, u_{t+1}, \ldots, x_T, \alpha_T, u_T)$ satisfies the linear time-varying dynamics (Assumption 1) and the risk-sensitivity level dynamics (Definition 5) under $\pi^*_t$ with the initialization $(x_{t+1}, \alpha_{t+1}) = (\bar{x}, \bar{\alpha})$. Consider $\pi^*_t = (\mu^*_t, \pi^*_t)$, where $\mu^*_t$ is a $\mathbb{X}$-Markov control law. Then, for any $(x_t, \alpha_t) = (x, \alpha) \in \mathbb{X}$, the following equalities hold:

$$\text{CVA}\text{R}^*_\alpha (\mu^*_t, \pi^*_t) (C_{t:T}|x_t = x)$$

(23)

where $C_{t+1:T}$ is conditioned on $x_{t+1} = f_t(x, u^*_t, d_t(\omega))$ in the integral above. Next, using the induction hypothesis and the definition of $G^*_{t}$ given by (19), we have:

$$\text{CVA}\text{R}^*_\alpha (C_{t+1:T}|x_t = x, u_t = u^*_t)$$

$$= \sup_{Z \in \mathcal{R}^*_\alpha (x, u^*_t)} \int_{\Omega} Z(\omega) \cdot \text{CVA}\text{R}^*_\alpha (C_{t+1:T}|x_{t+1}, \alpha T(\omega)) \mathbb{P}(d\omega)$$

$$= \sup_{Z \in \mathcal{R}^*_\alpha (x, u^*_t)} G^*_\alpha (Z, x, u^*_t).$$

The risk-sensitivity level at time $t + 1$ satisfies Definition 5 when using the policy $\pi^*_{t+1} = (\mu^*_{t+1}, \pi^*_{t+1})$. Indeed, this risk-sensitivity level is given by $\alpha_{t+1} = \alpha \cdot Z^*_t$, where $Z^*_t \in \arg \max G^*_t (Z, x, u^*_t)$ and $u^*_t = \mu^*_t(x, \alpha)$. Finally, combine the above equalities to obtain:

$$\text{CVA}\text{R}^*_\alpha (\mu^*_t, \pi^*_t) (C_{t:T}|x_t = x)$$

(23)

where equality (iii) holds since $\mu^*_t$ is a $\mathbb{X}$-Markov control law (Definition 4), and equality (iv) holds since $J_t = J^*_t$ (Theorem 2). Since the induction step has been shown, the proof is complete.

This concludes the theory portion of our paper. The remaining sections provide numerical examples, and our code is available at https://github.com/risk-sensitive-reachability/IEEE-TAC-2019.

**VI. NUMERICAL EXAMPLE: RISK-SENSITIVE SAFE SETS**

To illustrate our approach in a realistic setting, we provide a numerical example of a two-tank gravity-driven stormwater system with an automated valve (Fig. 2, Table I). Consider the following non-linear discrete-time dynamics model: $x_{t+1} = x_t + F(x_t, u_t, d_t(\omega)) \cdot \Delta t$ for $t = 0, 1, \ldots, T - 1$, where

$$F(x, u, d) = \begin{bmatrix} d - q_{\text{valve}}(x, u) - q_{\text{drain}}(x) \\ d + q_{\text{valve}}(x, u) - q_{\text{drain}}(x) \end{bmatrix}^T$$

where $q_{\text{valve}}(x, u) := u \cdot \pi^r_2 \cdot \text{sgn} h(x) \cdot \sqrt{2g|h(x)|}$ and $q_{\text{drain}}(x) := \begin{cases} C_a \pi^r_2 \cdot \sqrt{2g(x_2 - Z_2)} & \text{if } x_2 \geq Z_2 \\ 0 & \text{otherwise} \end{cases}$

and $x_t = [x_1, x_2]^T \in \mathbb{R}^2$ is the state vector, $x_t \in \mathbb{R}$ is the water level of tank $i$, $u_t \in [0, 1]$ is the valve setting (closed to open), $d_t \in \mathbb{R}$ is the random surface runoff (disturbance), and $\Delta t$ is the duration of $[t, t + 1]$. The constraint set $K := [0, K_1] \times [0, K_2]$ specifies the maximum water levels in the tanks. The stage cost $g_K(x_t) := \max(x_1 - K_1, x_2 - K_2, 0)$ is the maximum level of overflow when the system occupies state $x_t$. We identified a finite probability distribution for

4Here, the stormwater system is two-dimensional, whereas the system in our prior work [23] is one-dimensional. Moreover, an optimal policy for the system here is not known a priori, whereas an optimal policy for the system in [23] is known a priori.
Using the first three empirical moments of time-averaged runoff samples (Table II). The runoff samples were obtained by simulating a design storm in PCSWMM (Computational Hydraulics International), which extends USEPA’s Stormwater Management Model [39], [40].

We approximated \( \{U^*_\alpha\} \) by approximating \( J^*_0 \) on a grid of states and risk-sensitivity levels via Algorithm 1, and by utilizing the risk-sensitivity level interpolation approach proposed by [13], multi-linear interpolation of the state space, and uniform discretization of the action space. The values of \( \beta \) and \( \gamma \) from Theorem 1 were chosen empirically, where the magnitude of \( \gamma \) was constrained by the limitations of numerical solvers to manage differently scaled constraints. The computation time of the value functions \( J_0, J_1, \ldots, J_{T-1} \) and an optimal pre-commitment policy \( \pi_0^* = (\mu_0^*, \mu_1^*, \ldots, \mu_{T-1}^*) \) was about 230 hours for a three-dimensional grid of 50,490 nodes over \( T = 48 \) time points when run on a 4-core machine.\(^5\) Algorithm 1 was run serially on the state space grid, however at a given time point \( t \), the computations at each state are independent and can be run in parallel to reduce computation time. We approximated \( \{S^*_\alpha\} \) by performing 100,000 Monte Carlo simulations of \( \max\{g_k(x_k) : k = 0, 1, \ldots, T\} \) initialized at each \( x_0 = x \) in the state space grid under the policy computed by Algorithm 1, and by utilizing a consistent CVaR estimator [22, p. 300].

Numerical approximations of \( U^*_\alpha \) and \( S^*_\alpha \) (denoted by \( \hat{U}^*_\alpha \) and \( \hat{S}^*_\alpha \), respectively) for the stormwater system are shown in Fig. 3. Although the correctness of Algorithm 1 and the existence of optimal policies were formally proven for linear systems, we found that \( \hat{U}^*_\alpha \) provides an under-approximation of \( S^* \) when \( \beta e^{\gamma r} \) is sufficiently large, although Theorems 2 and 3 were proven for linear systems. Approximations of \( J_0(\cdot, \alpha) \) and \( W_0(\cdot, \alpha) \) are also provided. \( U^*_\alpha \) is the \( \beta e^{\gamma r} \)-sublevel set of \( J_0^*(\cdot, \alpha) = J_0(\cdot, \alpha) \) with \( (\beta, \gamma) = (2 \cdot 10^{-4}, 13) \). \( S^*_\alpha \) is the \( r \)-sublevel set of \( W_0^*(\cdot, \alpha) \).

\(^5\)The three-dimensional grid consists of 15 risk-sensitivity levels, 51 values of \( x_1 \), and 66 values of \( x_2 \) for a total of 50,490 nodes. To compute the value functions and an optimal pre-commitment policy, we ran Algorithm 1 in a cluster computing session that was allocated 4 CPU cores running at 2.8 GHz. We used the Tufts Linux Research Cluster (Medford, MA) running MATLAB (The Mathworks, Inc.) with MOSEK [44] and CVX [41], [42].

![Fig. 2. To illustrate our approach in a realistic setting, we develop a numerical example of a non-linear, two-tank stormwater system with an automated valve, where water flows by gravity between the tanks and can flow in either direction.](image)

![Fig. 3. Approximate contours of \( U^*_\alpha \) and \( S^*_\alpha \) (denoted by \( \partial \hat{U}^*_\alpha \) and \( \partial \hat{S}^*_\alpha \), respectively) are shown for \( \alpha \in \{0.099, 0.05, 0.01\} \) and \( r \in \{1, 2.5, 1.5\} \) for the (non-linear) stormwater system. These results indicate that our approach can be applied in a non-linear setting. \( U^*_\alpha \) provides an under-approximation of \( S^*_\alpha \) when \( \beta e^{\gamma r} \) is sufficiently large.\(^6\) These results indicate that Algorithm 1 is tractable on a realistic stochastic system.

**VII. CVaR versus Exponential Disutility**

Here we compare the Conditional Value-at-Risk criterion, \( J^*_0(13a) \), to the standard risk-sensitive criterion, which is expressed in terms of an exponential disutility function [19].

\(^6\)We found that \( U^*_\alpha \) provides an under-approximation of \( S^*_\alpha \) when \( \beta e^{\gamma r} \) is on the order of \( 10^{-4} \) or greater for \( \alpha \in \{0.099, 0.05, 0.01\} \). When \( \beta e^{\gamma r} \) is too small, numerical inaccuracies in the approximation of \( U^*_\alpha \) may be amplified by the transformation from \( J_0 \) to \( \frac{1}{\beta} \log(J_0/\beta) \leq r \). The numerical stability of the computations requires a careful selection of \( (\beta, \gamma) \) that balances the desire to make \( \gamma \) as large as possible with the understanding that \( \beta \) cannot be made arbitrarily small without introducing additional numerical issues.
The latter was developed to encode a preference for mean-variance-sensitive controllers by Peter Whittle in the early 1990s [19]. We provide relevant background from his seminal work [19] before showing our numerical results.

The (risk-averse) exponential disutility criterion $V_0^*(x, \theta) := \inf_{\pi} \frac{1}{\theta} \log \mathbb{E}^\pi \left( e^{\frac{1}{\theta} C_{0:T}|x_0 = x} \right)$

\[ = \inf_{\pi} \mathbb{E}^\pi (C_{0:T}|x_0 = x) - \frac{\theta}{2} V^\pi (C_{0:T}|x_0 = x) + O(\theta^2), \]

where the infimum is taken over a set of policies, $\theta \in (-1, 0)$ is the risk-sensitivity level, $x_0 = x \in X$ is the initial condition, and $C_{0:T}$ is the random cost of the state trajectory [19, Eqn. 1.10, Eqn. 1.11]. Equality (i) above holds since $0 < |\theta| < 1$. $\mathbb{E}^\pi(\cdot)$ and $V^\pi(\cdot)$ denote expectation and variance under the policy $\pi$, respectively. The range of $\theta$ encodes the risk-averse perspective that high variance is disadvantageous. If $\theta$ is closer to $-1$, then $V_0^*(\cdot, \theta)$ is more risk-averse; i.e., high variance is penalized more. However, if $\theta$ is closer to $0$, then $V_0^*(\cdot, \theta)$ is more risk-neutral; i.e., high variance is penalized less.

If $C_{0:T} := c_T(x_T) + \sum_{t=0}^{T-1} c_t(x_t, u_t)$, then the following algorithm computes $V_0^*(\cdot, \theta)$ and an optimal Markov policy under standard assumptions; see Remark 6, [19], and [30].

Algorithm 2 (Exp. Disutility Value Iteration [19], [30]):
Fix $\theta \in (-1, 0)$. Define the functions $V_{T-1}^\theta, \ldots, V_0^\theta$ recursively as follows: $\forall x \in X$ and $t = T-1, \ldots, 0$, $V_t^\theta(x) := \inf_{u \in U} \left\{ c_t(x, u) + \frac{1}{\theta} \log \mathbb{E} \left( e^{\frac{1}{\theta} V_{t+1}^\theta(f_t(x, u, d_t))} \right) \right\}$, with the terminal condition $V_T^\theta(x) := c_T(x)$, where the expectation is taken with respect to the distribution of $d_t$.

Remark 6: One can show that $V_0^*(\cdot, \theta) = V_0^\theta$. An optimal action at time $t$ when the system occupies the state $x_t = x$ is one that minimizes the objective function in (24). An optimal action is guaranteed to exist, if the objective in (24) is lower semi-continuous on $U$ and $U$ is compact.

Next, we use the stormwater system and a pedagogical thermal system to evaluate the CVaR criterion $J_0^\alpha(x, \alpha)$ relative to the exponential disutility criterion $V_0^\alpha(x, \theta)$ at different risk-sensitivity levels. The values $(\alpha, \theta) = (0.99, -0.01)$ encode a risk-neutral perspective, whereas the values $(\alpha, \theta) = (0.01, -0.99)$ encode a worst-case perspective. The values $(\alpha, \theta) = (0.01, -0.99)$ strike a balance between risk-neutral and worst-case by specifying a typical level of risk aversion.

### A. Stormwater System Example

We sampled $C_{0:T} := \sum_{t=0}^{T} \max(x_t - K_1, x_{t+1} - K_2)$ one million times from $x_0 \in [0, 1]^T$ using a policy synthesized with respect to the CVaR criterion for various $\alpha$ (Fig. 4, top row). We repeated this procedure for the exponential disutility criterion for various $\theta$ (Fig. 4, bottom row). The system that we consider is a realistic stormwater system that relies on gravity and a difference in hydraulic head to move water between the tanks. While the gravity-constrained maximum flow rate between the tanks can be modulated by the automated valve, its control authority is limited when compared with other active control options, such as pumps. Hence, when using the CVaR criterion, the CVaR $\alpha_{0.01}$, VaR $\alpha_{0.01}$, mean, and variance are only reduced by about 0.02, 0.02, 0.01, and 0.004, respectively, under a worst-case perspective versus a risk-neutral perspective (Fig. 4, top row).

### B. TCL System Example

Now, consider the following discrete-time thermally controlled load (TCL) system:

\[ x_{t+1} = ax_t + (1 - a)(b - \eta \theta R P u_t) + d_t, \quad t = 0, 1, \ldots, T - 1, \]

which we adopted from [10], and which was first developed by [43]. In the above model, $x_t \in \mathbb{R}$ is the temperature ($^\circ$C) of the thermal mass, $u_t \in [0, 1]$ is a continuous control input from no power to full power, and $d_t \in \mathbb{R}$ is a random disturbance due to environmental uncertainty (Table III).

The stage cost $g_t(x_t) := \max(x_t - 21, 20 - x_t)$ quantifies the extent of constraint violation of the state $x_t$ with respect to the constraint set $K = [20, 21]$ $^\circ$C. We discretized the action space $U = [0, 1]$ and the state space $X = [18, 23]$ $^\circ$C uniformly at a resolution of 0.1 and used linear interpolation of $X$ to implement Algorithms 1 and 2. We discretized the risk-sensitivity level space non-uniformly with more points near the levels of interest $\alpha \in \{0.99, 0.05, 0.01\}$ and utilized the risk-sensitivity level interpolation approach proposed by [13].

From two distinct initial conditions, we sampled $C_{0:T} := \sum_{t=0}^{T} \max(x_t - 21, 20 - x_t)$ one million times using a policy synthesized with respect to the CVaR criterion for various $\alpha$, and we repeated this procedure for the exponential disutility criterion for various $\theta$. We utilized the heavy-tailed finite probability distribution for $d_t$ called “Original” in Fig. 5 to train the policies and to generate the histograms of $C_{0:T}$ shown in Fig. 6 and Fig. 7. Further, we used the distribution for $d_t$ called “Perturbed” in Fig. 5 to generate the histograms of $C_{0:T}$ in Fig. 8 to assess robustness to distribution estimation error.

Our results show that the CVaR criterion minimizes the mean of higher-consequence outcomes, evident by reduced weight on the right-hand tail of the empirical distribution of $C_{0:T}$ as the degree of risk aversion increases (Fig. 6, top row, left to right). The exponential disutility criterion penalizes the mean and variance of $C_{0:T}$, and the empirical variance becomes smaller as the degree of risk aversion increases (Fig. 6, top row).
bottom row, left to right). While the exponential disutility criterion penalizes variance, this criterion is not guaranteed to minimize the mean of higher-consequence outcomes in the setting of asymmetric cost distributions (see estimated values of CVaR$_{0.01}$, top vs. bottom row, Fig. 6). Notably, at a typical level of risk aversion, the empirical variance of $C_{0:T}$ is smaller under the CVaR criterion compared to the exponential disutility criterion (Fig. 6, center column).

Our results indicate that the initial condition of the system impacts the relative advantage of using the CVaR criterion versus the exponential disutility criterion for policy synthesis. The probability distribution of the disturbance in the TCL impacts the relative advantage of using the CVaR criterion (Fig. 5), and the control input example represents a setting where the thermal mass is ex-

The probability distribution of the disturbance in the TCL impacts the relative advantage of using the CVaR criterion compared to the exponential disutility criterion (Fig. 6, center column).

**Remark 7:** Recall that $(\Omega, \mathcal{F}, \mathbb{P})$ is the probability space upon which the random disturbance $d_t$ is defined. The risk envelope $R^\alpha_{\pi}(x, u)$ is a subset of $L^2(\Omega, \sigma(f_t(x, u, d_t)), \mathbb{P})$, since it is a collection of $\mathbb{P}$-integrable, $\sigma(f_t(x, u, d_t))$-measurable bounded functions on $\Omega$ by definition (10). “Bounded” means bounded in $|| \cdot ||_\infty$, which implies bounded in $|| \cdot ||_2$. We study properties of the risk envelope in $L^2 := L^2(\Omega, \sigma(f_t(x, u, d_t)), \mathbb{P})$, since $L^2$ is reflexive and equals its dual, which simplifies proofs.

**Lemma 4 (Convexity and Continuity):** Fix $t$, $x_t = x \in X$, $u_t = u \in U$, and $\alpha_t = \alpha \in [0, 1]$. Define $H : R^\alpha_{\pi}(x, u) \times \Pi_{t+1} \to \mathbb{R}$ as follows:

$$H(Z, \pi) := \int_\Omega \frac{Z(\omega) \cdot \text{CVaR}^\alpha_{\pi}(Z(\omega))(C_{t+1:T}|x_t, u)}{\mathbb{P}(d\omega)}$$

where $C_{t+1:T}$ is conditioned on $x_{t+1} = f_t(x, u, d_t(\omega)) := Ax + B_t u + E_t d_t(\omega)$ in the integral above. Then, the following properties hold:

1) $H(Z, \cdot)$ is convex and continuous in the norm topology on $\Pi_{t+1}$ for any $Z \in R^\alpha_{\pi}(x, u)$.

2) $H(\cdot, \pi)$ is Lipschitz continuous in the relative norm topology on $R^\alpha_{\pi}(x, u) \subseteq L^2 := L^2(\Omega, \sigma(f_t(x, u, d_t)), \mathbb{P})$ for any $\pi \in \Pi_{t+1}$.

**Proof:** $C_{t+1:T}$ is convex on $\Pi_{t+1}$ since $C_{t+1:T}$ is a convex function, the state trajectory is affine on $\Pi_{t+1}$, and the composition of a convex function with an affine function is convex. Further, $H(Z, \cdot)$ is convex on $\Pi_{t+1}$ for any $Z \in R^\alpha_{\pi}(x, u)$ because $C_{t+1:T}$ is convex on $\Pi_{t+1}$. Conditional Value-at-Risk is a convex functional, $Z(\omega) \geq 0$ for almost every $\omega \in \Omega$, and expectation is a linear functional.

Define the product norm on $\Pi_{t+1}$ as the maximum uniform norm, i.e., $||| \pi ||| := \max(|||\mu_k||| : k = t + 1, \ldots, T - 1)$. Take $\{\pi(n)\}$ in $\Pi_{t+1}$ converging to $\pi$ in $\Pi_{t+1}$. Fix $r > 0$, define $\gamma_n := |||\pi - \pi(n)|||$, and define $\tilde{\pi}(n) \in \Pi_{t+1}$ so that $\pi = \gamma_n \tilde{\pi}(n) + (1 - \gamma_n)\pi_n$. Fix $Z \in R^\alpha_{\pi}(x, u)$. Since $H(Z, \cdot)$ is convex on $\Pi_{t+1}$,

$$H(Z, \pi) \leq \gamma_n H(Z, \tilde{\pi}(n)) + (1 - \gamma_n) H(Z, \pi(n)).$$

As $n \to \infty$, $\gamma_n H(Z, \tilde{\pi}(n)) \to 0$, since $H(Z, \cdot)$ is bounded and $\gamma_n \to 0$. So, $H(Z, \pi) \leq \lim \inf H(Z, \pi(n))$, which shows lower semi-continuity. To show upper semi-continuity, i.e., $\lim \sup H(Z, \pi(n)) \leq H(Z, \pi)$, define $\tilde{\pi}(n) \in \Pi_{t+1}$ so that $\pi(n) = \gamma_n \tilde{\pi}(n) + (1 - \gamma_n)\pi_n$. Use convexity to obtain $H(Z, \pi(n)) \leq \gamma_n H(Z, \tilde{\pi}(n)) + (1 - \gamma_n) H(Z, \pi)$, and take the limit superior as $n \to \infty$.

Now, fix $\pi \in \Pi_{t+1}$ and $\omega \in \Omega$. Use the definition of CVaR (1) as an integral over VaR if $\alpha Z(\omega) > 0$ and as an essential supremum if $\alpha Z(\omega) = 0$ to show that $Z(\omega) \to Z(\omega) \cdot \text{CVaR}^\alpha_{\pi}(\omega)(C_{t+1:T}|x_t, u) = f_t(x, u, d_t(\omega))$ is Lipschitz continuous on $\mathbb{R}$ for almost every $\omega \in \Omega$; set the Lipschitz constant equal to the essential supremum of $C_{t+1:T}$. Since $\int_\Omega |Z(\omega)|^2 \mathbb{P}(d\omega) := |||Z|||_1^2 \leq |||Z|||_2^2$ for any $Z \in R^\alpha_{\pi}(x, u)$, $H(\cdot, \pi)$ is Lipschitz continuous in the relative norm topology on $R^\alpha_{\pi}(x, u) \subset L^2$ for any $\pi \in \Pi_{t+1}$.}

**APPENDIX I**

Here we show two results that are required to prove the minimax equality (Lemma 2). Lemma 4 states that an expected CVaR is the cost of the state trajectory is convex and continuous on the policy space and is continuous on the risk envelope. Lemma 5 specifies important topological properties of the risk envelope.
Lemma 5 (Properties of Risk Envelope): Fix $t$, $x_t = x \in X$, $u_t = u \in U$, and $\alpha_t = \alpha \in [0, 1]$. $R^\alpha_t(x, u)$, as defined by (10), is a non-empty, convex, and compact set in $L^2 := L^2(\Omega, \sigma\{f_t(x, u, d_t)\}, \mathbb{P})$ endowed with the weak topology.

Proof: $R^\alpha_t(x, u)$ is non-empty, since it contains $Z(\omega) = 1$ for almost every $\omega \in \Omega$. $R^\alpha_t(x, u) \subset L^2$, since bounded random variables have bounded second moments. So, $R^\alpha_t(x, u)$ is bounded in $|| \cdot ||_2$, $R^\alpha_t(x, u)$ is a convex subset of $L^2$ by inspection. Since only bounded costs are evaluated in our setting, for any $\alpha \in [0, 1]$, CVar$_\alpha$ is a real-valued coherent risk measure on $L^2$. Moreover, for any $\alpha \in [0, 1]$ and $Y \in L^2$ such that $Y$ is bounded, the following equality holds by [22, Thm. 6.4, Eqn. 6.40, Eqn. 6.70]: CVar$_\alpha(Y) = \sup_{Z \in R^\alpha_t(x, u)} \int \Omega Z(\omega)Y(\omega)\mathbb{P}(d\omega)$. So, $R^\alpha_t(x, u)$ is closed in the weak$^*$ topology on $L^2$ by [22, Thm. 6.6, p. 264]. Finally, a bounded and weakly$^*$ closed set is weakly$^*$ compact by the Banach-Alaoglu Theorem [22, Thm. 7.70, p. 401]. Thus, $R^\alpha_t(x, u)$ is compact in the weak$^*$ topology on $L^2$. Since $L^2$ is reflexive, the weak and the weak$^*$ topologies on $L^2$ coincide, hence $R^\alpha_t(x, u)$ is compact in the weak topology on $L^2$. ■

Remark 8: $L^2$ endowed with the weak topology is a locally convex topological vector space, since the weak topology in a topological vector space is locally convex [33, p. 161].

APPENDIX II

Here we provide three results that facilitate the synthesis of optimal pre-commitment policies (Section V). Lemmas 6 and 7 are required to prove the existence of X-Markov control laws. Lemma 8 is critical for ensuring that the risk-sensitivity level
would be lower semi-continuous in $G$ expectation preserves lower semi-continuity, continuous bounded function is lower semi-continuous.) Since $Z$, then $(Z(\omega), u) \rightarrow J_{t+1}^*(f_t(x, u, d_t(\omega)), \alpha Z(\omega)) = J_{t+1}^*(f_t(x, u, d_t(\omega)), \alpha Z(\omega))$ would be lower semi-continuous for almost every $\omega \in \Omega$, since a lower semi-continuous function composed with a continuous function is lower semi-continuous. Then, $(Z(\omega), u) \rightarrow Z(\omega) \cdot J_{t+1}^*(f_t(x, u, d_t(\omega)), \alpha Z(\omega))$ would be lower semi-continuous for almost every $\omega \in \Omega$, since $Z(\omega)$ is nonnegative and bounded for almost every $\omega \in \Omega$. (The product of a nonnegative, continuous bounded function and a lower semi-continuous bounded function is lower semi-continuous.) Since expectation preserves lower semi-continuity, $G_t^\alpha(Z, x, u)$ would be lower semi-continuous in $(Z, x, u)$ to complete the proof. So, it suffices to show that $J_{t+1}^*$ is lower semi-continuous on $X$, which is shown in Lemma 7 below. 

**Lemma 7 (Lower Semi-Continuity of $J_t^*$):** Fix $t$. $J_t^*$, as defined in (13a), is lower semi-continuous on $X = X \times [0, 1]$. 

**Proof:** Recall that each $J_t^*$ is bounded since the stage costs and the terminal cost are bounded. It suffices to show that $J_t$, as defined in (11), is lower semi-continuous on $X$ by Theorem 2. We proceed by induction. Let $(x, \alpha) \in X$. $J_T(x, \alpha) = c_T(x)$, which is continuous. Now, assume $J_{t+1}^*$ is lower semi-continuous on $X$ for some $t$. Since $U$ is compact, $c_t$ is continuous, and lower semi-continuity is preserved through summation, it suffices to show that the following (bounded) map $(x, \alpha, u) \mapsto \sup_{\omega \in \Omega} G_t^\alpha(Z, x, u)$ is lower semi-continuous on $X \times U$ by [32, Prop. D.5 (b)], where $G_t^\alpha(Z, x, u) = \int_\Omega Z(\omega) \cdot J_{t+1}^*(f_t(x, u, d_t(\omega)), \alpha Z(\omega)) \, d\omega$ by Theorem 2. Since $(x, \alpha, u) \mapsto \sup_{\omega \in \Omega} G_t^\alpha(Z, x, u)$ is a lower semi-continuous set-valued mapping by Assumption 2, if $G_t^\alpha(Z, x, u)$ is lower semi-continuous in $(Z, x, \alpha, u)$, then the desired result holds by [38, Lemma 3.2 (a)]. Since $(x, u) \mapsto f_t(x, u, d_t(\omega))$ is continuous for almost every $\omega \in \Omega$ by Assumption 1, $(Z(\omega), x, \alpha, u) \mapsto (f_t(x, u, d_t(\omega)), \alpha Z(\omega))$ is continuous for almost every $\omega \in \Omega$. Since $J_{t+1}^*$ is lower semi-continuous on $X$ by the induction hypothesis, $(Z(\omega), x, \alpha, u) \mapsto J_{t+1}^*(f_t(x, u, d_t(\omega)), \alpha Z(\omega))$ is lower semi-continuous for
almost every \( \omega \in \Omega \). Moreover, since \( Z(\omega) \) is nonnegative and bounded for a.e. \( \omega \in \Omega \), \( (Z(\omega), x, \alpha, u) \mapsto Z(\omega) \cdot J_{t+1}(f_t(x, u, d_t(\omega)), \alpha Z(\omega)) \) is lower semi-continuous for almost every \( \omega \in \Omega \). Since expectation preserves lower semi-continuity, the proof is complete.

**Lemma 8**: \( G^t_t (\cdot, x, u) \) is USC on Risk Envelope: Fix \( t, x_t = x \), \( u_t = u \), and \( \alpha_t = \alpha \). \( G^t_t (\cdot, x, u) \), as defined by (19), is upper semi-continuous in the relative weak topology on \( \mathcal{R}^t_t (x, u) \subset L^2 \). The authors gratefully acknowledge many fruitful discussions with Zhiyan Ding and Michael Lim.

**REFERENCES**

[1] D. P. Bertsekas and I. B. Rhodes, “On the Minimax Reachability of Target Sets and Target Tubes,” *Automatica*, vol. 7, no. 2, pp. 233–247, 1971.

[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, 2005.
[3] K. Margellos and J. Lygeros, “Hamilton-Jacobi formulation for reach-avoid differential games,” IEEE Transactions on Automatic Control, vol. 56, no. 8, pp. 1849–1861, 2011.

[4] M. Chen, et al., “Decomposition of reachable sets and tubes for a class of nonlinear systems,” IEEE Transactions on Automatic Control, vol. 63, no. 11, pp. 3675–3688, 2018.

[5] M. Chen and C. J. Tomlin, “Hamilton-Jacobi reachability: Some recent theoretical advances and applications in unmanned airspace management,” Annual Review of Control, Robotics, and Autonomous Systems, vol. 1, no. 1, pp. 333–358, 2018.

[6] A. Abate, et al., “Probabilistic reachability and safety for controlled discrete time stochastic hybrid systems,” Automatica, vol. 44, no. 11, pp. 2724–2734, 2008.

[7] S. Summers and J. Lygeros, “Verification of discrete time stochastic hybrid systems: A stochastic reach-avoid decision problem,” Automatica, vol. 46, no. 12, pp. 1951–1961, 2010.

[8] M. Kamgarpour, et al., “Discrete time stochastic hybrid dynamical games: Verification and controller synthesis,” in IEEE Conference on Decision and Control and European Control Conference (CDC-ECC), 2011, pp. 6122–6127.

[9] J. Ding, et al., “A stochastic games framework for verification and control of discrete time stochastic hybrid systems,” Automatica, vol. 49, pp. 2665–2674, 2013.

[10] I. Yang, “A dynamic game approach to distributionally robust safety specifications for stochastic systems,” Automatica, vol. 94, pp. 94–101, 2018.

[11] S. Samuelson and I. Yang, “Safety-Aware Optimal Control of Stochastic Systems Using Conditional Value-at-Risk,” in American Control Conference (ACC), 2018, pp. 6285–6290.

[12] T. Osogami, “Robustness and Risk-Sensitivity in Markov Decision Processes,” in Advances in Neural Information Processing Systems, 2012, pp. 233–241.

[13] Y. Chow, et al., “Risk-Sensitive and Robust Decision-Making: a CVaR Optimization Approach,” in Advances in Neural Information Processing Systems, 2015, pp. 1522–1530.

[14] V. Borkar and R. Jain, “Risk-constrained Markov decision processes,” IEEE Transactions on Automatic Control, vol. 59, no. 9, pp. 2574–2579, 2014.

[15] W. B. Haskell and R. Jain, “A convex analytic approach to risk-aware Markov decision processes,” SIAM Journal on Control and Optimization, vol. 53, no. 3, pp. 1569–1598, 2015.

[16] S. Stanko, “Risk-Averse Distributional Reinforcement Learning,” M.S. thesis, Computer Science, Czech Technical University, Prague, Czech Republic, 2018. [Online] Available: https://dspace.cvut.cz/bitstream/handle/10467/76432/F3-DP-2018-Stanko-Silvstris-thesis.pdf?sequence=-1&isAllowed=y

[17] A. Hakobyan, G. C. Kim, and I. Yang, “Risk-Aware Motion Planning and Control Using CVaR-Constrained Optimization,” IEEE Robotics and Automation Letters, vol. 4, no. 4, pp. 3924–3931, 2019.

[18] S. Singh, et al., “A framework for time-consistent, risk-sensitive model predictive control: Theory and algorithms,” IEEE Transactions on Automatic Control, vol. 64, no. 7, pp. 2905–2912, 2019.

[19] P. Whittle, Risk-sensitive Optimal Control, Chichester: Wiley, 1990.

[20] J. Kisiala, “Conditional Value-at-Risk: Theory and Applications,” M.S. thesis, Operational Research, University of Edinburgh, Edinburgh, Scotland, 2015. [Online] Available: https://www.maths.ed.ac.uk/~prichtar/docs/Kisiala_Dissertation.pdf

[21] R. T. Rockafellar and S. Uryasev, “Conditional value-at-risk for general loss distributions,” Journal of Banking & Finance, vol. 26, no. 7, pp. 1443–1471, 2002.

[22] A. Shapiro, D. Dentcheva, and A. Ruszczyński, Lectures on Stochastic Programming: Modeling and Theory, Society for Industrial and Applied Mathematics, Mathematical Programming Society, 2009.

[23] M. P. Chapman, et al., “A Risk-Sensitive Finite-Time Reachability Approach for Safety of Stochastic Dynamic Systems,” American Control Conference (ACC), 2019.

[24] C. W. Miller and I. Yang, “Optimal control of conditional value-at-risk in continuous time,” SIAM Journal on Control and Optimization, vol. 55, no. 2, pp. 856–884, 2017.

[25] G. C. Pflug and A. Pichler, “Time-inconsistent multistage stochastic programs: Martingale bounds,” European Journal of Operational Research, vol. 249, no. 1, pp. 155–163, 2016.

[26] G. C. Pflug and A. Pichler, “Time-consistent decisions and temporal decomposition of coherent risk functionals,” Mathematics of Operations Research, vol. 41, no. 2, pp. 682–699, 2016.

[27] A. Akametalu, “A learning-based approach to safety for uncertain robotic systems,” Ph.D. thesis, Electrical Engineering and Computer Sciences, University of California Berkeley, USA, 2018. [Online] Available: www2.eecs.berkeley.edu/Pubs/TechRpts/2018/EERCS-2018-41.html

[28] P. Artzner, et al., “Coherent multiperiod risk adjusted values and Bellmans principle,” Annals of Operations Research, vol. 152, no. 1, pp. 5–22, 2007.

[29] A. Shapiro, “On a time consistency concept in risk averse multistage stochastic programming,” Operations Research Letters, vol. 37, no. 3, pp. 143–147, 2009.

[30] D. P. Bertsekas, Dynamic Programming and Optimal Control, vol. 1, 4th ed., Belmont: Athena Scientific, 2017.

[31] S. Boyd and L. Vandenberghe, Convex Optimization, Cambridge: Cambridge University Press, 2004.

[32] O. Hernández-Lerma and J. B. Lasserre, Discrete-Time Markov Control Processes: Basic Optimality Criteria, New York: Springer, 1996.

[33] R. B. Ash, Real Analysis and Probability, New York: Academic Press, 1972.

[34] B. Ricceri and S. Simons, Minimax Theory and Applications, Dordrecht: Kluwer Academic Publishers, 1998.

[35] V. Barbu and T. Precupanu, Convexity and Optimization in Banach Spaces, 4th ed., Dordrecht: Springer, 2012.

[36] A. Shapiro, “Interchangeability principle and dynamic equations in risk averse stochastic programming,” Operations Research Letters, vol. 45, no. 4, pp. 377–381, 2017.

[37] A. Ruszczyński, “Risk-averse dynamic programming for Markov decision processes,” Mathematical Programming, vol. 125, no. 2, pp. 235–261, 2010.

[38] J. I. González-Trejo, O. Hernández-Lerma, and L. F. Hoyos-Reyes, “Minimax control of discrete-time stochastic systems,” SIAM Journal on Control and Optimization, vol. 41, no. 5, pp. 1626–1659, 2002.

[39] M. P. Chapman, et al., “Reachability Analysis as a Design Tool for Stormwater Systems,” in IEEE Conference on Technologies for Sustainability (SusTech), pp. 1–8, 2018.

[40] 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.

[41] M. C. Grant and S. P. Boyd, CVX: Matlab Software for Disciplined Convex Programming, Version 2.1, 2014. [Online] Available: http://cvxr.com/cvx

[42] M. C. Grant and S. P. Boyd, “Graph implementations for nonsmooth convex programs,” In Recent Advances in Learning and Control, pp. 95–110, London: Springer, 2008. [Online] Available: http://stanford.edu/~boyd/graph_dcp.html

[43] R. E. Mortensen and K. P. Haggerty, “A stochastic computer model for heating and cooling loads,” IEEE Transactions on Power Systems, vol. 3, no. 3, pp. 1213–1219, 1988.

[44] MOSEK ApS. The MOSEK optimization toolbox for MATLAB manual, Version 9.0, 2019. [Online] Available: http://docs.mosek.com/9.0/toolbox/index.html

[45] P. M. Esfahani, et al., “From infinite to finite programs: Explicit error bounds with applications to approximate dynamic programming,” SIAM Journal on Optimization, vol. 28, no. 3, pp. 1968–1998, 2018.

[46] M. Korda and I. Mezić, “Linear predictors for nonlinear dynamical systems: Koopman operator meets model predictive control,” Automatica, vol. 93, pp. 149–160, 2018.
Shafiqul Islam is a Ph.D. candidate advised by Dr. Claire Tomlin in Electrical Engineering and Computer Sciences (EECS) at the University of California Berkeley. He is grateful to be a recipient of the Fulbright Scholarship, the NSF Graduate Research Fellowship, and the Berkeley Fellowship for Graduate Study. He earned her B.S. degree (with Distinction) and her M.S. degree in Mechanical Engineering from Stanford University. Margaret’s research lies at the intersection of stochastic and robust optimal control theory. She is particularly interested in developing decision-making algorithms that protect against rare events with applications to practical design and management of safety-critical systems. Margaret is delighted to be a participant of 2019 Rising Stars in EECS hosted by the University of Illinois Urbana–Champaign, and she aims to become a professor at a research-focused university in the United States or Canada.

Kevin Smith is a Ph.D. candidate in Environmental and Water Resources Engineering at Tufts University and a recipient of the NSF Integrative Graduate Education and Research Traineeship (IGERT) on Water and Diplomacy. Kevin also works as a product developer at OptiRTC, Inc., where he is responsible for developing flexible real-time systems for the continuous monitoring and adaptive control of stormwater infrastructure. Kevin earned his B.A. in Environmental Studies from Oberlin College and his B.S. in Earth and Environmental Engineering from Columbia University. Kevin’s research seeks to understand the opportunities and risks associated with semi-autonomous civil infrastructure when considered as a technology for mediating environmental conflicts. Kevin recently co-edited a research manuscript on interdisciplinary approaches to addressing complex water issues, *Interdisciplinary Collaboration for Water Diplomacy: A Principled and Pragmatic Approach*, with his advisor Dr. Shafiqul Islam.

Margaret Chapman is a Ph.D. candidate advised by Dr. Claire Tomlin in Electrical Engineering and Computer Sciences (EECS) at the University of California Berkeley. She is grateful to be a recipient of the Fulbright Scholarship, the NSF Graduate Research Fellowship, and the Berkeley Fellowship for Graduate Study. She earned her B.S. degree (with Distinction) and her M.S. degree in Mechanical Engineering from Stanford University. Margaret’s research lies at the intersection of stochastic and robust optimal control theory. She is particularly interested in developing decision-making algorithms that protect against rare events with applications to practical design and management of safety-critical systems. Margaret is delighted to be a participant of 2019 Rising Stars in EECS hosted by the University of Illinois Urbana–Champaign, and she aims to become a professor at a research-focused university in the United States or Canada.

Yuxi Han is a Ph.D. candidate in Mathematics at the University of Wisconsin–Madison. She earned her M.S. degree in Statistics from George Washington University in 2016 and spent the next two years studying mathematics at the University of California Berkeley. She focuses her research and study on partial differential equations, especially viscosity solutions to Hamilton-Jacobi equations and their connections to dynamical systems. She aims to become a professor at a research-focused university in the United States or China.

Dr. Marco Pavone is an Associate Professor of Aeronautics and Astronautics at Stanford University, where he is the Director of the Autonomous Systems Laboratory. Before joining Stanford, he was a Research Technologist within the Robotics Section at the NASA Jet Propulsion Laboratory. He received a Ph.D. degree in Aeronautics from the Massachusetts Institute of Technology in 2010. His main research interests are in the development of methodologies for the analysis, design, and control of autonomous systems, with an emphasis on self-driving cars, autonomous aerospace vehicles, and future mobility systems. He is a recipient of a number of awards, including a Presidential Early Career Award for Scientists and Engineers (PECASE), an Office of Naval Research Young Investigator Award, a National Science Foundation Early Career (CAREER) Award, a NASA Early Career Faculty Award, and an Early-Career Spotlight Award from the Robotics Science and Systems Foundation. He was identified by the American Society for Engineering Education (ASEE) as one of America’s 20 most highly promising investigators under the age of 40. He is currently serving as an Associate Editor for the IEEE Control Systems Magazine.

Dr. Insoon Yang is an Assistant Professor of Electrical and Computer Engineering at Seoul National University (SNU). He received B.S. degrees in Mathematics and in Mechanical Engineering (summa cum laude) from SNU in 2009; and an M.S. in EECS, an M.A. in Mathematics and a Ph.D. in EECS from UC Berkeley in 2012, 2013 and 2015, respectively. He was an Assistant Professor of Electrical and Computer Engineering at University of Southern California from 2016 to 2018, and a Postdoctoral Associate at the Laboratory for Information and Decision Systems in Massachusetts Institute of Technology from 2015 to 2016. His research interests are in stochastic control and optimization, and reinforcement learning, with application to cyber-physical systems and safe autonomy. He is a recipient of the 2015 Eli Jury Award and a finalist for the Best Student Paper Award at the 55th IEEE Conference on Decision and Control 2016. He is an associate editor of the IEEE CSS Conference Editorial Board.

Dr. Claire Tomlin is the Charles A. Desoer Professor of Engineering in EECS at Berkeley. She was an Assistant, Associate, and Full Professor in Aeronautics and Astronautics at Stanford from 1998 to 2007, and in 2005 joined Berkeley. Claire works in the area of control theory and hybrid systems, with applications to air traffic management, UAV systems, energy, robotics, and systems biology. She is a MacArthur Foundation Fellow (2006), an IEEE Fellow (2010), in 2017 she was awarded the IEEE Transportation Technologies Award, and in 2019 was elected to the National Academy of Engineering and the American Academy of Arts and Sciences.