Safe Stochastic Model Predictive Control

T. Brüdigam, R. Jacumet, D. Wollherr, and M. Leibold

Abstract—Combining efficient and safe control for safety-critical systems is challenging. Robust methods may be overly conservative, whereas probabilistic controllers require a trade-off between efficiency and safety. In this work, we propose a safety algorithm that is compatible with any stochastic Model Predictive Control method for linear systems with additive uncertainty and polytopic constraints. This safety algorithm uses the control inputs of a stochastic Model Predictive Control as long as a safe backup planner can ensure safety with respect to satisfying hard constraints subject to bounded uncertainty. Besides ensuring safe behavior, the proposed stochastic Model Predictive Control algorithm guarantees recursive feasibility and input-to-state stability of the system origin. The benefits of the safe stochastic Model Predictive Control algorithm are demonstrated in a numerical simulation, highlighting the advantages compared to purely robust or stochastic predictive controllers.

I. INTRODUCTION

Designing controllers for safety-critical systems requires considering two major challenges. Safety must be ensured for a system subject to uncertainty, and the controller should reduce conservatism to enable efficient system behavior, i.e., maximizing desired objectives. As it is possible to define safety via input and state constraints, Model Predictive Control (MPC) is a suitable method to control safety-critical systems subject to uncertainty.

Robust Model Predictive Control (RMPC) handles system uncertainty in a robust, but conservative way [1], [2], where tube-based MPC is the most common approach [3]–[5]. Stability and recursive feasibility guarantees are possible if the uncertainty bound is known initially. RMPC has successfully been applied to safety-critical applications such as automated driving [6], [7], autonomous racing [8], and robotic manipulation [9].

Stochastic Model Predictive Control (SMPC) reduces conservatism by employing chance constraints [10], [11]. Chance constraints allow for a small probability of constraint violation, reducing the impact of unlikely worst-case uncertainty realizations. Multiple SMPC approaches exist to determine a tractable reformulation of the probabilistic chance constraint, e.g., analytical reformulations based on normal distributions [12], sampling based approaches [13], [14], affine disturbance feedback approaches [15], or tube-based approaches [16]. Applications to safety-critical systems mainly focus on automated driving [17]–[20]. However, whereas applying these SMPC approaches yields efficient trajectories, safety is not guaranteed as the chance constraint allows for a non-zero collision probability.

Safety within SMPC is specifically addressed in [21] for automated vehicles. This failsafe SMPC approach uses a failsafe backup predictive controller, which guarantees that the next SMPC input may be safely applied, ensuring safe SMPC trajectories for automated driving. Further approaches have recently been proposed to address safety within MPC. A combination of MPC and control barrier functions allows considering safety similarly to how Lyapunov functions are used for stability [22], [23]. However, guaranteeing recursive feasibility in the presence of uncertainty remains a challenge. An MPC approach to minimize constraint violation probability is proposed in [24], but the method is only applicable if norm-based constraints can be employed. In [25], [26] a predictive safety filter is proposed to guarantee safety in probability for reinforcement learning. This is achieved by enforcing that only those reinforcement learning-based inputs may be applied, which allow for satisfaction of a soft-constrained optimal control problem (OCP).

In this work, we propose an SMPC safety algorithm for linear systems with additive uncertainty and polytopic constraints. This general safety algorithm significantly extends the approach in [21], which only considered one specific SMPC approach designed for automated vehicles. The safety algorithm of this work guarantees safety (satisfying all constraints) by employing a backup controller, which ensures that applying the first optimized SMPC input allows still finding a safe backup trajectory in the following step. The key contributions are as follows. The key contributions are as follows.

- We provide a safety algorithm compatible with any SMPC for linear systems with additive uncertainty and polytopic constraints. Furthermore, the risk parameter of the SMPC does not influence safety, and no terminal constraint is required in the SMPC OCP.
- We guarantee recursive feasibility of the safety algorithm and, in contrast to [21], we ensure input-to-state stability of the system origin.

With the proposed safety algorithm of this work, for a given safety-critical application and based on desired control objectives, the most suitable SMPC approach can be chosen. This choice may be made independently of required properties, which are later ensured by the proposed safety algorithm. The proposed method combines advantages of stochastic and robust predictive control. These advantages of the proposed safe SMPC algorithm are demonstrated in a simulation example, including comparisons to pure SMPC.
and pure RMPC.

This work is structured as follows. Section II introduces the problem. The safe SMPC framework and its properties are presented in Sections III and IV. A simulation example and conclusive remarks are given in Sections V and VI.

Notation: Regular letters indicate scalars, bold lowercase letters denote vectors, and bold uppercase letters are used for matrices, e.g., \( a, \alpha, A \), respectively. The probability of event \( \mathcal{A} \) is denoted by \( \Pr(\mathcal{A}) \). The sets of integers and real numbers are given by \( \mathbb{Z} \) and \( \mathbb{R} \), respectively. The closed interval between integers \( a \) and \( b \) is denoted by \( [a, b] \). Absolute values and norms are indicated by \( |a| \) and \( ||a||_A^2 = A^T a A \). A function \( \gamma \) is of class \( K \) if \( \gamma \) is positive definite and strictly increasing. A function \( \alpha \) is of class \( K_\infty \) if \( \alpha \) is of class \( K \) and unbounded. Within an OCP, the state \( x_{t+k|t} \) denotes the prediction for step \( t+k \) obtained at time step \( t \). We define the set addition \( A \oplus B := \{ a + b | a \in A, b \in B \} \) and set subtraction \( A \ominus B := \{ x \in \mathbb{R}^n | \{ x \} \ominus B \subseteq A \} \).

II. Problem Setup

We consider a linear, discrete-time system

\[
x_{t+1} = Ax_t + Bu_t + Gw_t = f(x_t, u_t, w_t)
\]

with states \( x_t \in \mathbb{R}^{n_x} \), inputs \( u_t \in \mathbb{R}^{n_u} \), and uncertainties \( w_t \in \mathbb{R}^{n_w} \) at time step \( t \), as well as the known matrices \( A, B, \) and \( G \) with appropriate dimensions. System (1) is subject to input constraints \( u_t \in U \) and state constraints \( x_t \in \mathcal{X} \).

Assumption 1 (Uncertainty): The uncertainty \( w_t \) is independent and identically distributed and bounded by \( w_t \in \mathcal{W} \).

The general task is to minimize an objective function

\[
J(x_t, U_t) = \sum_{k=0}^{N-1} l(x_{t+k|t}, u_{t+k|t}) + V_f(x_{t+N|t})
\]

with prediction horizon \( N \), stage cost \( l \), disturbance-free nominal state \( x_{t+k|t} \), and the terminal cost function \( V_f \) while satisfying input and state constraints. In SMPC, this is achieved by repeatedly solving an OCP \( \mathcal{P}(x_t) \), i.e.,

\[
\min_{U_t} J(x_t, U_t) \quad \text{s.t. } x_{t+k|t} = f(x_{t+k|t}, u_{t+k|t}, w_{t+k|t}) \quad \forall k = 0, \ldots, N-1
\]

This work is structured as follows. Section II introduces the problem. The safe SMPC framework and its properties are presented in Sections III and IV. A simulation example and conclusive remarks are given in Sections V and VI.

A. Property Definitions

If SMPC is employed in safety-critical applications, three properties are required. First, safety must be ensured. Second, if the SMPC is feasible at a time step, a solution must also exist at the next time step, known as recursive feasibility. Third, the closed-loop system behavior must be stable. Definitions to ensure these properties are given in the following.

Definition 1 (Robustly Positively Invariant Set): A set \( \mathcal{X}_0 \) is robustly positively invariant for a system \( f(x_t, u_t, w_t) \) if for all \( x_0 \in \mathcal{X}_0 \subseteq \mathcal{X} \) it holds that \( f^+(x_t, u_t, w_t) \in \mathcal{X}_0 \), \( \forall w_t \in \mathcal{W}, \forall t \geq 0 \).

Definition 2 (Robustly Control Invariant Set): A set \( \mathcal{X}_0 \) is robustly control invariant for a system \( f(x_t, u_t, w_t) \) if for all \( x_0 \in \mathcal{X}_0 \subseteq \mathcal{X} \) it holds that \( \exists u_t = u(x_t) \in U \) such that \( f(x_t, u_t, w_t) \in \mathcal{X}_0, \forall w_t \in \mathcal{W}, \forall t > 0 \).

Definition 3 (Safety): For a system \( f(x_t, u_t, w_t) \) the state \( x_t \), \( t \geq 0 \), is safe if \( x_t \in \mathcal{X}_0 \subseteq \mathcal{X} \) where \( \mathcal{X}_0 \) is robustly control invariant for system \( f(x_t, u_t, w_t) \).

Definition 4 (Recursive Feasibility): A feasible MPC at \( t = 0 \) that remains feasible for all \( t > 0 \) is recursively feasible.

Definition 5 (Input-to-State Stability [15]): The origin of a system \( f^+(x, w) \) is input-to-state stable (ISS) with region of attraction \( \mathcal{X}_0 \subseteq \mathbb{R}_{x}^n \) that contains the origin if \( \mathcal{X}_0 \) is robustly positively invariant and if there exist a continuous function \( V : \mathcal{X}_0 \rightarrow \mathbb{R}_{\geq 0} \) and functions \( \alpha_1, \alpha_2, \alpha_3 \in \mathcal{K}_\infty, \gamma \in \mathcal{K} \) such that for all \( x \in \mathcal{X}_0 \) and \( w \in \mathcal{W} \)

\[
\alpha_1(||x||) \leq V(x) \leq \alpha_2(||x||) \quad (4a)
\]

\[
V(f^+(x, w)) - V(x) \leq -\alpha_3(||x||) + \gamma(||w||). \quad (4b)
\]

Then, function \( V \) is called an ISS Lyapunov function. If the origin of a system is ISS, it is guaranteed that the change in \( V \) is bounded as long as the uncertainty is bounded. If the uncertainty is zero, the origin of an ISS system is asymptotically stable with region of attraction \( \mathcal{X}_0 \).

B. Problem Statement

The aim of this work is to design a safety algorithm for SMPC that exploits the advantage of reduced conservatism in SMPC while ensuring the previously described properties. Objective 1: A safety algorithm for the SMPC OCP (3) must guarantee safety (Definition 3), recursive feasibility (Definition 4), and stability (Definition 5).

In the following, we propose an SMPC algorithm including a safe backup (predictive) controller that ensures satisfaction of all requirements listed in Objective 1.

III. Safe Stochastic MPC

A. General Safe SMPC Algorithm

SMPC allows for a certain probability of constraint violation. Therefore, in order to use SMPC in a safe way, it needs to be ensured that applying an SMPC input allows for robust constraint satisfaction in subsequent time steps.

We propose a general safe SMPC algorithm that consists of an SMPC part and a backup predictive controller. This safe SMPC algorithm, shown in Figure 1, yields an input
At each time step $t$, which is determined based on the following two modes:

- **Stochastic mode** (with OCP $P^s(x_t)$)
- **Backup mode** (with OCP $P^b(x_t)$)

We now present details on the two OCPs and on which mode to apply.

1) **SMPC Optimal Control Problem:** We consider the general SMPC OCP $P^s(x_t)$ with horizon $N$ given by

$$
\min_{\hat{U}_t} J(x_t, \hat{U}_t)
$$

subject to

$$
x_{t+k+1|t} = f(x_{t+k|t}, u_{t+k|t}, w_{t+k|t})
$$

$$
x_{t+k+1|t} = f(x_{t+k|t}, u_{t+k|t}, 0)
$$

$$
u_{t+k|t} \in U, \quad k \in I_{0:N-1}
$$

$$
\Pr(x_{t+k|t} \in X) \geq \beta, \quad k \in I_{1:N}
$$

$$
x_{t|t} = x_t, \quad \hat{x}_{t|t} = x_t
$$

yielding the optimal input sequence $\hat{U}_t^* = (u_{t|t}^*, \ldots, u_{t+N-1|t}^*)$ with the SMPC control law $u_t^*(x_t) = u_{t|t}^*$. Any SMPC method may be used to reformulate the chance constraint (5c) into a tractable formulation, depending on the uncertainty distribution.

2) **Backup MPC Optimal Control Problem:** We consider a backup MPC controller with horizon $N^b$ and OCP $P^b(x_t)$ with cost function $J^b(x_t, U_t^b)$, yielding the optimal cost $J^b(x_t, U_t^{b*})$ with input sequence $U_t^{b*} = (u_{t|t}^{b*}, \ldots, u_{t+N^b-1|t}^{b*})$, and control law $u_t^b(x_t) = u_{t|t}^{b*}$, resulting in the closed-loop system

$$
x_{t+1} = f(x_t, u_t^b(x_t), w_t)
$$

for system (1). Various backup controllers are possible in this algorithm, given that they fulfill the following assumption.

**Assumption 2 (Backup MPC):** The backup MPC OCP $P^b(x_t)$, with value function $J^b$ and control law $u_t^b(x_t)$, is chosen such that $P^b(x_t)$ is recursively feasible, $x_t \in X$ and $u_t \in U$ for all $t$, and such that the origin of the closed-loop system (6) is ISS with region of attraction $X_0$, where $X_0$ is robust positively invariant for all $w_t \in W$.

Various MPC schemes exist that fulfill Assumption 2, as discussed in Section III-B.

The safe SMPC algorithm only applies SMPC inputs if it is guaranteed that the backup OCP $P^b(x_t)$ may still be solved at the next time step. Applying the first SMPC input $u_t^s(x_t)$ to the nominal system yields the next nominal state

$$
x_{t+1} = Ax_t + Bu_t^s(x_t).
$$

It is guaranteed that the backup OCP is feasible for any first step uncertainty $w_t \in W$ if

$$
x_{t+1} \in X_0 \cap W
$$

where $X_0 = X_0 \cap W$, which ensures that $x_{t+1} \in X_0$.

3) **Safe SMPC Modes:** We are now able to propose two different modes within the safe SMPC algorithm, evaluated at time step $t$.

- **Stochastic Mode:** The control law $u_t = u_t^s(x_t)$ is applied if the SMPC OCP is feasible and if (8) is fulfilled, i.e., $U_t^{s*} \neq \emptyset$ and $x_{t+1}^* \in X_0$.

- **Backup Mode:** If the SMPC OCP is infeasible or if (8) is not satisfied, i.e., $U_t^{s*} = \emptyset$ or $x_{t+1}^* \notin X_0$, the backup MPC OCP is solved and the control law $u_t = u_t^b(x_t)$ is applied.

Note that in the stochastic mode, only one OCP is solved, whereas the backup mode requires solving a second OCP.

Safety could also be guaranteed by adding a robust safety constraint to the SMPC OCP, however, the proposed method makes it possible to use the less conservative SMPC solution as long as possible. This potentially leads to environment changes so that the robust OCP solution never needs to be applied. Consider the example of a car attempting to change lanes into a tight gap. For a robust approach, the gap may be too tight to start a maneuver. With the proposed method, SMPC initiates the maneuver while a safe backup trajectory to the original lane still exists. By starting the maneuver, other vehicles may increase the gap size so that the maneuver can be completed safely by only applying SMPC inputs.

**B. MPC Details**

The proposed algorithm allows for handling of any SMPC approach to solve (5), e.g., SMPC with exact chance constraint reformulations based on normal distributions, affine disturbance feedback SMPC, or sampling-based SMPC. A suitable SMPC method may be chosen depending on the type of uncertainty and the type of system.

Assumption 2 allows employing various MPC schemes for the backup controller, which enables application of a wider class of backup controllers compared to [21]. The most intuitive choice are RMPC approaches that guarantee recursive feasibility and stability for a bounded uncertainty. The backup MPC can also be based on other approaches, such as MPC based on reachability analysis [27] or the failsafe MPC idea described in [21]. It is even possible to consider recursively feasible SMPC approaches as backup controllers, e.g., [16], if Assumption 2 may be satisfied.
IV. PROPERTIES

In the following, we show that the proposed SMPC algorithm is recursively feasible, safe, and ISS.

A. Recursive Feasibility

Based on Definition 4, we first prove recursive feasibility of the OCP of the safe SMPC algorithm described in Section III-A.

Theorem 1 (Recursive Feasibility): Let Assumptions 1 and 2 hold and let the system input \( u_t \) be determined based on the proposed safe SMPC algorithm in Section III-A. Let \( x_0 \in X_0 \) at the initial time step \( t = 0 \). Then, the safe SMPC algorithm remains feasible for \( t \geq 0 \) as the backup OCP \( P^b(x_t) \) remains feasible.

Proof: If \( P^a(x_t) \) is feasible, i.e., \( U^a_t \neq \emptyset \), and \( x_{t+1}^* \in X_0 \cap \mathcal{W} \), then \( u_t = u^a(x_t) \) ensures that \( x_{t+1}^* \in X_0 \), which guarantees that a solution \( U^b_{t+1} \) exists for \( P^b(x_{t+1}) \).

In the backup mode, \( U^b_{t+1} \) exists for \( P^b(x_t) \) as \( x_t \in X_0 \) and Assumption 2 ensures that \( P^b(x_{t+1}) \) remains feasible.

Hence, all possibilities are covered. This holds for all \( t \geq 0 \).

B. Safety

We require that the safe SMPC algorithm described in Section III-A is safe. Based on Definition 3, this requirement demands that all constraints are met at all time steps, which we show in the following.

Theorem 2 (Safety): Let Assumptions 1 and 2 hold and let the system input \( u_t \) be determined based on the proposed safe SMPC algorithm in Section III-A. Then, for a safe initial state \( x_0 \in X_0 \), safety according to Definition 3 is guaranteed for \( t > 0 \).

Proof: The proof is based on Theorem 1; hence, it is guaranteed that one of the two modes is applicable at each time step \( t \). In the stochastic mode, \( u_t = u^a(x_t) \) is only applied if \( x_{t+1}^* \in X_0 \cap \mathcal{W} \), yielding \( x_{t+1}^* \in X_0 \). The backup mode guarantees, by design, that \( x_{t+1}^* \in X_0 \). Therefore, \( x_t \in X_0 \) for \( t > 0 \).

As shown, safety is ensured by the backup predictive controller and (8), despite SMPC allowing for constraint violations in the open-loop prediction.

C. Stability

In MPC, stability is often proved by showing that the value function is decreasing for subsequent time steps, also known as the descent property. These proofs are based on the MPC idea of a moving horizon, where the previously planned input sequence remains valid and only one additional input element is added to the input sequence for the next time step. For the proposed safe SMPC algorithm, however, this assumption does not hold. Since switching between different modes is possible, the predicted input and state trajectories may vary at each time step. We tackle this challenge by using an ISS result from [15, Lemma 22], which we repeat in the following lemma.

Lemma 1 (Lipschitz ISS Lyapunov Function [15]): Let \( f : X_0 \times W \to \mathbb{R}^n \) be Lipschitz continuous on \( X_0 \times \mathcal{W} \). Let \( X_0 \subset \mathbb{R}^n \) contain the origin and be a robust positively invariant set for the function \( f(x, u) \). Let there exist a Lipschitz continuous function \( V : X_0 \to \mathbb{R} \) such that for all \( x \in X_0 \)

\[
\alpha_1(||x||) \leq V(x) \leq \alpha_2(||x||) \quad (9a)
\]

\[
V(f(x, u)) - V(x) \leq -\alpha_3(||x||) \quad (9b)
\]

with functions \( \alpha_1, \alpha_2, \alpha_3 \in \mathcal{C}_\infty \). Then, \( V \) is an ISS Lyapunov function and the origin is ISS for system \( f(x, u) \) with region of attraction \( X_0 \).

Lemma 1 ensures that the origin of a system subject to uncertainty is ISS if the undisturbed system is asymptotically stable and the system is Lipschitz continuous with respect to state \( x \) and uncertainty \( w \).

Assumption 3 (Backup MPC Cost): The cost function \( J^b \) is selected according to (2). The stage cost is chosen as

\[
l(x_{t+k|t}, u_{t+k|t}) = ||x_{t+k|t}||_Q + ||u_{t+k|t}||_R \quad \text{with } Q = Q^T > 0, R = R^T > 0, \text{ and the nominal states } x_{t+k|t}.
\]

The terminal cost \( V_t(x_{t+N|t}) \) is chosen as a Lyapunov function in a terminal set \( X_f \) for the undisturbed nominal closed-loop system \( x_{t+1} = (A + BK)x_t \) such that for all \( x_t \in X_f \) it holds that

\[
V_t((A + BK)x_t) - V_t(x_t) \leq -x_t^T(Q + K^TRK)x_t \quad (10)
\]

where \( K \) is a stabilizing feedback matrix.

We can now formulate the ISS property of a system controlled with the proposed algorithm.

Theorem 3 (ISS for Safe SMPC): Let Assumptions 1-3 hold and let the system input \( u_t \) be determined based on the proposed safe SMPC algorithm in Section III-A. Then, for \( x_0 \in X_0 \), the origin is ISS for system (1) and \( x_t \in X_0 \), \( t > 0 \).

Proof: We prove ISS by showing that \( V(x_t) = J^b(x_t) \) is an ISS Lyapunov function for (1) where \( V(\cdot) \) satisfies (9a) and (9b). Any input prediction in either of the two modes can be described by \( u'_{t+k|t} = u^a_{t+k|t} - \tilde{u}_{t+k|t} \), \( k \in [0, N-1] \) where \( \tilde{u}_{t+k|t} \) represents the offset between the backup MPC input element \( u^b_{t+k|t} \) and the input element obtained in the safe SMPC algorithm \( u^b_{k+1|t} \). As \( u'_{t+k|t} \) and \( u^b_{t+k|t} \) are bounded, \( \tilde{u}_{t+k|t} \) is bounded, allowing to define the new bounded uncertainty \( \tilde{w}_{t+k|t} = (\tilde{u}_{t+k|t}, w_{t+k|t})^T \). This yields the closed loop system

\[
f(x_t, u_t, w_t) = Ax_t + Bu_t + Gw_t \quad (11a)
\]

\[
= Ax_t + Bu^b(x_t) - B\tilde{u}_t + Gw_t \quad (11b)
\]

\[
= Ax_t + Bu^b(x_t) + [-B, G]\tilde{w}_t \quad (11c)
\]

which can be abbreviated by \( f'(x_t, \tilde{w}_t) \).
Function \( f' \) is continuous and \( f'(0, 0) = 0 \). With Assumption 3, it holds that \( V(\cdot) \) is positive definite and continuous on \( X_0 \). Hence, based on [29, Lemma 4.3], functions \( \alpha_1, \alpha_2 \in K_{\infty} \) exist such that \( \alpha_1(||x_t||) \leq V(x_t) \leq \alpha_2(||x_t||) \), i.e., (9a) is fulfilled.

Due to Assumption 2, \( V(x_t) = J^{\beta^*} \) is an ISS Lyapunov function for the undisturbed system with \( \tilde{w}_t = 0 \), i.e., \( V(f'(x_t, 0)) - V(x_t) \leq -\alpha_3(||x_t||) \). With \( J^{\beta} \) designed according to Assumption 3 and a bounded \( X_0 \), \( J^{\beta^*} \) is Lipschitz continuous. Hence, Lemma 1 is fulfilled and \( V(\cdot) \) is an ISS Lyapunov function for \( f'(x_t, \tilde{w}_t) \) with \( x_t \in X_0 \), i.e., it holds that \( V(f'(x_t, \tilde{w}_t)) - V(x_t) \leq -\alpha_3(||x_t||) + \gamma(||\tilde{w}_t||) \). Hence, the origin is ISS with the safe SMPC algorithm.

Note that tuning the risk parameter in the SMPC OCP does not impact recursive feasibility, safety, or stability. This allows choosing a risk parameter that yields the most efficient behavior.

**V. Numerical Results**

We analyze the proposed algorithm in a numerical example, based on [16], and elaborate on the advantages over SMPC and RMPC. Simulations are carried out in Matlab where the set calculations are done with the Multi-Parametric Toolbox 3 [30] and the MPC routine is based on [31].

**A. Simulation Setup**

We consider the discrete-time system

\[
\begin{align*}
  x_{t+1} &= \begin{bmatrix} 1 & 0.0075 \\ -0.143 & 0.996 \end{bmatrix} x_t + \begin{bmatrix} 4.798 \\ 0.115 \end{bmatrix} u_t + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} w_t
\end{align*}
\]

(12)

with \( x = (x_1, x_2)^T \) and the normally distributed uncertainty \( w \sim \mathcal{N}(0, \Sigma_w) \), \( w_t \in \mathcal{W} \) where \( \Sigma_w = \text{diag}(0.06, 0.06) \) and \( \mathcal{W} = \{w_t | ||w_t||_\infty \leq 0.07\} \). The input is bounded by \( ||u_t|| \leq 0.2 \) and we employ the state constraint \( x_1 \leq 2.8 \). Additionally, we define \( ||x_1|| \leq 10 \) and \( ||x_2|| \leq 10 \) to obtain a bounded set \( \mathcal{X} \), however, in the following simulation only \( x_1 \leq 2.8 \) is regarded. The initial state is \( x_0 = (-1.3, 3.5)^T \).

For the SMPC OCP, we approximate the uncertainty with the non-truncated normal distribution \( w \sim \mathcal{N}(0, \Sigma_w) \) and split the state into a deterministic and a probabilistic part \( x_t = z_t + e_t \), yielding an adapted input \( u_t = K(z_t + e_t) \) with a stabilizing feedback matrix \( K \) and the new input decision variable \( \nu_t \). The state constraint is considered as the chance constraint \( \Pr(x_1 \in 2.8) \geq \beta \) with \( \beta = 0.8 \). The normal distribution \( w \) allows for the chance constraint reformulation

\[
\begin{align*}
  x_{1,k} \leq 2.8 - \gamma_{cc,k}
\end{align*}
\]

(13a)

\[
\begin{align*}
  \gamma_{cc,k} = \sqrt{2(1, 0)^T \Sigma_x^k(1, 0) \text{erf}^{-1}(2\beta - 1)}
\end{align*}
\]

(13b)

with the inverse error function \( \text{erf}^{-1}(.) \) and the error covariance matrix \( \Sigma_x^{k+1} = \Phi \Sigma_x^k \Phi^T + \Sigma_w \) with \( \Sigma_w = \text{diag}(0, 0) \) and \( \Phi = A + BK \).

For the backup MPC, we use an RMPC approach according to [32], satisfying Assumption 2. This approach yields the tightened state constraint \( \pi_1 \leq 1.72 \) and tightened input constraint \( -0.018 \leq \pi_i \leq 0.025 \). The terminal constraint \( \lambda_t \) is chosen to be a maximal robust control invariant set.

For SMPC and RMPC, we employ a sampling time \( \Delta t = 0.1 \), a horizon \( N = N^b = 11 \), and we use the stabilizing feedback gain \( K = [-0.29, 0.49] \).

For both the Assumption 3 with \( \tilde{w}_t = 0 \), \( J^{b^*} \) is Lipschitz continuous. Hence, Lemma 1 is fulfilled and \( V(\cdot) \) is an ISS Lyapunov function for \( f'(x_t, \tilde{w}_t) \) with \( x_t \in X_0 \), i.e., it holds that \( V(f'(x_t, \tilde{w}_t)) - V(x_t) \leq -\alpha_3(||x_t||) + \gamma(||\tilde{w}_t||) \). Hence, the origin is ISS with the safe SMPC algorithm.

Note that tuning the risk parameter in the SMPC OCP does not impact recursive feasibility, safety, or stability. This allows choosing a risk parameter that yields the most efficient behavior.

**V. Numerical Results**

We analyze the proposed algorithm in a numerical example, based on [16], and elaborate on the advantages over SMPC and RMPC. Simulations are carried out in Matlab where the set calculations are done with the Multi-Parametric Toolbox 3 [30] and the MPC routine is based on [31].

**A. Simulation Setup**

We consider the discrete-time system

\[
\begin{align*}
  x_{t+1} &= \begin{bmatrix} 1 & 0.0075 \\ -0.143 & 0.996 \end{bmatrix} x_t + \begin{bmatrix} 4.798 \\ 0.115 \end{bmatrix} u_t + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} w_t
\end{align*}
\]

(12)

with \( x = (x_1, x_2)^T \) and the normally distributed uncertainty \( w \sim \mathcal{N}(0, \Sigma_w) \), \( w_t \in \mathcal{W} \) where \( \Sigma_w = \text{diag}(0.06, 0.06) \) and \( \mathcal{W} = \{w_t | ||w_t||_\infty \leq 0.07\} \). The input is bounded by \( ||u_t|| \leq 0.2 \) and we employ the state constraint \( x_1 \leq 2.8 \). Additionally, we define \( ||x_1|| \leq 10 \) and \( ||x_2|| \leq 10 \) to obtain a bounded set \( \mathcal{X} \), however, in the following simulation only \( x_1 \leq 2.8 \) is regarded. The initial state is \( x_0 = (-1.3, 3.5)^T \).

For the SMPC OCP, we approximate the uncertainty with the non-truncated normal distribution \( w \sim \mathcal{N}(0, \Sigma_w) \) and split the state into a deterministic and a probabilistic part \( x_t = z_t + e_t \), yielding an adapted input \( u_t = K(z_t + e_t) \) with a stabilizing feedback matrix \( K \) and the new input decision variable \( \nu_t \). The state constraint is considered as the chance constraint \( \Pr(x_1 \in 2.8) \geq \beta \) with \( \beta = 0.8 \). The normal distribution \( w \) allows for the chance constraint reformulation

\[
\begin{align*}
  x_{1,k} \leq 2.8 - \gamma_{cc,k}
\end{align*}
\]

(13a)

\[
\begin{align*}
  \gamma_{cc,k} = \sqrt{2(1, 0)^T \Sigma_x^k(1, 0) \text{erf}^{-1}(2\beta - 1)}
\end{align*}
\]

(13b)

with the inverse error function \( \text{erf}^{-1}(.) \) and the error covariance matrix \( \Sigma_x^{k+1} = \Phi \Sigma_x^k \Phi^T + \Sigma_w \) with \( \Sigma_w = \text{diag}(0, 0) \) and \( \Phi = A + BK \).

For the backup MPC, we use an RMPC approach according to [32], satisfying Assumption 2. This approach yields the tightened state constraint \( \pi_1 \leq 1.72 \) and tightened input constraint \( -0.018 \leq \pi_i \leq 0.025 \). The terminal constraint \( \lambda_t \) is chosen to be a maximal robust control invariant set.
The proposed algorithm is not limited to SMPC. Instead of using SMPC, other controllers, e.g., learning-based methods, can be used. This would allow ensuring safety and stability for learning-based controllers.

ACKNOWLEDGEMENT

The authors thank Francesco Borrelli and Sarah Buhlmann for the collaboration and valuable discussions. This work was supported by a fellowship within the IFI program of the German Academic Exchange Service (DAAD) and the Bavaria California Technology Center (BaCaTeC) grant 1-[2020-2].

REFERENCES

[1] A. Bemporad and M. Morari. Robust model predictive control: A survey, pages 207–226. Springer London, London, 1999.
[2] D.Q. Mayne, J.B. Rawlings, C.V. Rao, and P.O.M. Scokaert. Constrained model predictive control: Stability and optimality. Automatica, 36(6):789 – 814, 2000.
[3] W. Langson, I. Chryssostomidis, S.V. Rakovic, and D.Q. Mayne. Robust model predictive control using tubes. Automatica, 40(1):125 – 133, 2004.
[4] D.Q. Mayne, E.C. Kerrigan, E.J. van Wyk, and P. Falugi. Tube-based robust nonlinear model predictive control. International Journal of Robust and Nonlinear Control, 21(11):1341–1353, 2011.
[5] J. Köhler, R. Soloperto, M.A. Müller, and F. Allgöwer. A computationally efficient robust model predictive control framework for uncertain nonlinear systems. IEEE Transactions on Automatic Control, 66(2):794–801, 2021.
[6] Y. Gao, A. Gray, H.E. Tseng, and F. Borrelli. A tube-based robust nonlinear predictive control approach to semi-autonomous ground vehicles. Vehicle System Dynamics, 52(6):802–823, 2014.
[7] M. Lorenzen, F. Dabbene, R. Tempo, and F. Allgoewer. Constraint-robust model predictive control. In Control Conference (ECC), pages 811–817, 2019.
[8] A. Wischnewski, M. Euler, S. Günnis, and B. Lohmann. Tube model predictive control for an autonomous race car. Vehicle System Dynamics, 0(0):1–23, 2021.
[9] J. Nubert, J. Köhler, V. Berenz, F. Allgöwer, and S. Trimpe. Safe and fast tracking on a robot manipulator: Robust mpc and neural network control. IEEE Robotics and Automation Letters, 5(2):3050–3057, 2020.
[10] A. Mesbah. Stochastic model predictive control: An overview and perspectives for future research. IEEE Control Systems, 36(6):30–44, Dec 2016.
[11] M. Farina, L. Giuliani, and R. Scattolini. Stochastic linear model predictive control with chance constraints – a review. Journal of Process Control, 44(Supplement C):53 – 67, 2016.
[12] M. Farina, L. Giuliani, L. Magni, and R. Scattolini. An approach to output-feedback mpc of stochastic linear discrete-time systems. Automatica, 55:140–149, 2015.
[13] L. Blackmore, M. Ono, A. Bektasov, and B.C. Williams. A probabilistic particle-control approximation of chance-constrained stochastic predictive control. Trans. Rob., 26(3):502–517, June 2010.
[14] G. Schilbach, L. Fagiano, C. Frei, and M. Morari. The scenario approach for stochastic model predictive control with bounds on closed-loop constraint violations. Automatica, 50(12):3099 – 3018, 2014.
[15] P.J. Goulart, E.C. Kerrigan, and J.M. Maciejowski. Optimization over state feedback policies for robust control with constraints. Automatica, 42(4):523–533, 2006.
[16] M. Lorenzen, F. Dabbene, R. Tempo, and F. Allgöwer. Constraint-tightening and stability in stochastic model predictive control. IEEE Transactions on Automatic Control, 62(7):3165–3177, July 2017.
[17] A. Carvalho, Y. Gao, S. Lefevere, and F. Borrelli. Stochastic predictive control of autonomous vehicles in uncertain environments. In 12th Int. Symposium on Advanced Vehicle Control, Tokyo, Japan, 2014.
[18] G. Cesari, G. Schilbach, A. Carvalho, and F. Borrelli. Scenario model predictive control for lane change assistance and autonomous driving on highways. IEEE Intelligent Transportation Systems Magazine, 9(3):23–35, Fall 2017.
