mathematics

MDPI

Article

Safeness Index-Based Economic Model Predictive Control of Stochastic Nonlinear Systems

Zhe Wu [1], Helen Durand [2] and Panagiotis D. Christofides [1,3,*]

[1] Department of Chemical and Biomolecular Engineering, University of California, Los Angeles, CA 90095-1592, USA; wuzhe@g.ucla.edu
[2] Department of Chemical Engineering and Materials Science, Wayne State University, Detroit, MI 48202, USA; helen.durand@wayne.edu
[3] Department of Electrical and Computer Engineering, University of California, Los Angeles, CA 90095-1592, USA
* Correspondence: pdc@seas.ucla.edu

Received: 28 March 2018; Accepted: 27 April 2018; Published: 3 May 2018

Abstract: Process operational safety plays an important role in designing control systems for chemical processes. Motivated by this, in this work, we develop a process Safeness Index-based economic model predictive control system for a broad class of stochastic nonlinear systems with input constraints. A stochastic Lyapunov-based controller is first utilized to characterize a region of the state-space surrounding the origin, starting from which the origin is rendered asymptotically stable in probability. Using this stability region characterization and a process Safeness Index function that characterizes the region in state-space in which it is safe to operate the process, an economic model predictive control system is then developed using Lyapunov-based constraints to ensure economic optimality, as well as process operational safety and closed-loop stability in probability. A chemical process example is used to demonstrate the applicability and effectiveness of the proposed approach.

Keywords: process operational safety; economic model predictive control; Safeness Index; nonlinear systems; chemical processes; probabilistic uncertainty

1. Introduction

Process operational safety has become crucially important in the chemical industry since the failure of process safety devices/human error often leads to disastrous incidents causing human and capital loss [1]. Motivated by this, recently, a new class of economic model predictive control systems (EMPC), in which the cost function penalizes process economics instead of the distances from the steady-state in a general quadratic form, was utilized to account for process operational safety and economic optimality based on a function called the Safeness Index [2,3]. These new EMPC methods complement previous efforts on economic model predictive control (e.g., [4–7]), which were not concerned explicitly with process operational safety. Specifically, in [2], a Safeness Index function that indicates the level of safety of a given state was utilized to characterize a safe operating region and used as a constraint in the EMPC design such that the closed-loop state of a nonlinear process is guaranteed to be driven into the safe operating region in finite time in the presence of sufficiently small bounded disturbances and, if the Safeness Index takes a special form related to a Lyapunov function used in the EMPC design, to never again exit that safe operating region while maximizing the economics of the process. However, in general, the Safeness Index does not have to take this special form and may therefore leave the safe operating region for finite periods of time (this may be acceptable depending on how the notion of a "safe" region of operation is selected; e.g., perhaps a "safe" region of operation means it is safe to operate in for all times, but that if the state is not in that region for short periods of time, there is not an immediate concern). Therefore, with a general form

of the Safeness Index, the hard constraint on this function in the EMPC design of [2] with a Safeness Index-based constraint may not be feasible. Due to the potential infeasibility issue caused by the hard constraint, the potential for the state to leave the safe operating region unless the Safeness Index has a specific form and the fact that disturbances may not be sufficiently small to guarantee that the closed-loop state re-enters this safe operating region, the EMPC design with a Safeness Index-based constraint may be limited in terms of its applicability to stochastic nonlinear systems.

On the other hand, MPC and EMPC of stochastic nonlinear systems have received a lot of attention recently (e.g., [8,9]). Uncertainty in the process model may be considered to have a worst-case upper and lower bound, or it may be considered to have unbounded variation and therefore be treated in a probabilistic manner. Since the variation of disturbances is not bounded in a stochastic nonlinear system, the Lyapunov-based economic model predictive control (LEMPC) framework [4] developed for nonlinear systems with small bounded disturbances is unable to guarantee closed-loop stability (i.e., the state of the closed-loop system stays within a well-characterized region of the state-space); instead, probabilistic closed-loop stability results are expected in this case. To that end, in [10], the Markov-chain Monte Carlo technique was used to derive the probabilistic convergence to a near-optimal solution for a constrained stochastic optimization problem. In [9], a Lyapunov-based model predictive control (LMPC) method was proposed for stochastic nonlinear systems to drive the state to a steady-state within an explicitly characterized region of attraction in probability. Recently, the work [11] developed a Lyapunov-based EMPC method for stochastic nonlinear systems by utilizing the probability distribution of the disturbance term to derive closed-loop stability and recursive feasibility results in probability.

In the same direction, this work focuses on the design of Safeness Index-based economic model predictive control systems for a broad class of stochastic nonlinear systems with input constraints. Specifically, under the assumption of the stabilizability of the origin of the stochastic nonlinear system via a stochastic Lyapunov-based control law, a process Safeness Index function and the level sets of multiple Lyapunov functions are first utilized to characterize a safe operating region in state-space, starting from which recursive feasibility and process operational safety are derived in probability for the stochastic nonlinear system under an economic model predictive controller. This economic model predictive control method is then designed that utilizes stochastic Lyapunov-based constraints to achieve economic optimality, as well as feasibility and process operational safety in probability in the well-characterized safe operating region.

The rest of the manuscript is organized as follows: in the Preliminaries, the notation, the class of systems and the stabilizability assumptions are given. In the Main Results, the process Safeness Index and the Safeness Index-based LEMPC are introduced. Subsequently, the Safeness Index-based LEMPC using multiple level sets of Lyapunov functions (to broaden the state-space set for which it is recursively feasible) is developed for the nominal system. Based on this, the corresponding stochastic Safeness Index-based LEMPC and its probabilistic process operational safety and feasibility properties are developed for the nonlinear stochastic system. Finally, a nonlinear chemical process example is used to demonstrate the application of the proposed stochastic Safeness Index-based LEMPC.

2. Preliminaries

2.1. Notations

Throughout the paper, we use the notation $(\Omega, \mathcal{F}, \mathbf{P})$ to denote a probability space. The notation $|\cdot|$ is used to denote the Euclidean norm of a vector, and the notation $|\cdot|_Q$ denotes the weighted Euclidean norm of a vector (i.e., $|x|_Q = x^T Q x$ where Q is a positive definite matrix). x^T denotes the transpose of x. $\mathbf{R}_+$ denotes the set $[0, \infty)$. The notation $L_f V(x)$ denotes the standard Lie derivative $L_f V(x) := \frac{\partial V(x)}{\partial x} f(x)$. Given a set $\mathcal{D}$, we denote the boundary of $\mathcal{D}$ by $\partial\mathcal{D}$, the closure of $\mathcal{D}$ by $\overline{\mathcal{D}}$ and the interior of $\mathcal{D}$ by $\mathcal{D}^o$. Set subtraction is denoted by "\", i.e., $A \backslash B := \{x \in \mathbf{R}^n : x \in A, x \notin B\}$. A continuous function $\alpha : [0, a) \to [0, \infty)$ is said to be a class $\mathcal{K}$ function if $\alpha(0) = 0$ and it is strictly

increasing. The function $f(x)$ is said to be a class C^k function if the i-th derivative of f exists and is continuous for all $i = 1, 2, ..., k$. Consider a stochastic process $x(t, w) : [0, \infty) \times \Omega \to \mathbf{R}^n$ on $(\Omega, \mathcal{F}, \mathbf{P})$. For each $w \in \Omega$, $x(\cdot, w)$ is a realization or trajectory of the stochastic process, and we abbreviate $x(t, w)$ as $x_w(t)$. $\mathbf{E}(A)$, $\mathbf{P}(A)$, $\mathbf{E}(A \mid \cdot)$ and $\mathbf{P}(A \mid \cdot)$ are the expectation, the probability, the conditional expectation and the conditional probability of the occurrence of the event A, respectively. The hitting time τ_X of a set X is the first time that the state trajectory hits the boundary of X. Additionally, we define $\tau_{X,T}(t) = \min\{\tau_X, T, t\}$, where T is the operation time.

2.2. Class of Systems

Consider a class of continuous-time stochastic nonlinear systems described by the following system of stochastic differential equations:

$$dx(t) = f(x(t))dt + g(x(t))u(t)dt + h(x(t))dw(t) \tag{1}$$

where $x \in \mathbf{R}^n$ is the stochastic state vector and $u \in \mathbf{R}^m$ is the input vector. The available control action is defined by $U := \{u \in \mathbf{R}^m \mid u_i^{\min} \leq u \leq u_i^{\max}, i = 1, 2, ..., m\}$. The disturbance $w(t)$ is a standard q-dimensional independent Wiener process defined on the probability space $(\Omega, \mathcal{F}, \mathbf{P})$. $f(\cdot)$, $g(\cdot)$, and $h(\cdot)$ are sufficiently smooth vector and matrix functions of dimensions $n \times 1$, $n \times m$ and $n \times q$, respectively. It is assumed that the steady-state of the system with $w(t) \equiv 0$ is $(x_s^*, u_s^*) = (0, 0)$. The initial time t_0 is defined as zero ($t_0 = 0$). We also assume that $h(0) = 0$ such that the disturbance term $h(x(t))dw(t)$ of Equation (1) vanishes at the origin.

Definition 1. *Given a C^2 Lyapunov function $V : \mathbf{R}^n \to \mathbf{R}_+$, the infinitesimal generator ($\mathcal{L}V$) of the system of Equation (1) is defined as follows:*

$$\mathcal{L}V(x) = L_f V(x) + L_g V(x)u + \frac{1}{2} Tr\{h(x)^T \frac{\partial^2 V}{\partial x^2} h(x)\} \tag{2}$$

We assume that $L_f V(x)$, $L_g V(x)$ and $h(x)^T \frac{\partial^2 V}{\partial x^2} h(x)$ are locally Lipschitz throughout the work.

Definition 2. *Assuming that the equilibrium of the uncontrolled system $dx(t) = f(x(t))dt + h(x(t))dw(t)$ is at the origin, then the origin is said to be asymptotically stable in probability, if for any $\epsilon > 0$, the following conditions hold ([12]):*

$$\lim_{x(0) \to 0} \mathbf{P}(\lim_{t \to \infty} x(t) = 0) = 1 \tag{3a}$$

$$\lim_{x(0) \to 0} \mathbf{P}(\sup_{t \geq 0} |x(t)| > \epsilon) = 0 \tag{3b}$$

Proposition 1. *Given the uncontrolled system $dx(t) = f(x(t))dt + h(x(t))dw(t)$, if for all $x \in D_0 \subset \mathbf{R}^n$, where D_0 is an open neighborhood of the origin, $\mathcal{L}V < 0$ holds $\forall t \in (0, \infty)$, then $\mathbf{E}(V(x(t))) < V(x(0))$, $\forall t \in (0, \infty)$, and the origin of the uncontrolled system is asymptotically stable in probability ([12]).*

2.3. Stabilizability Assumptions

We assume there exists a stochastic stabilizing feedback control law $u = \Phi_s(x) \in U$ (e.g., [13,14]) such that the origin of the system of Equation (1) can be rendered asymptotically stable in probability for all $x \in D \subset \mathbf{R}^n$, where D is an open neighborhood of the origin, in the sense that there exists a positive definite C^2 stochastic control Lyapunov function V that satisfies the following inequality:

$$\begin{aligned} \mathcal{L}V &= L_f V(x) + L_g V(x)\Phi_s(x) + \frac{1}{2} Tr\{h^T \frac{\partial^2 V}{\partial x^2} h\} \\ &\leq -\alpha_1(|x|) \end{aligned} \tag{4}$$

where $\alpha_1(\cdot)$ is a class $\mathcal{K}$ function.

Based on the controller $\Phi_s(x)$, we characterize the set $\phi_d := \{x \in \mathbf{R}^n \mid \mathcal{L}V + \kappa V(x) \leq 0, u = \Phi_s(x) \in U, \kappa > 0\}$. We also choose a level set $\Omega_\rho := \{x \in \phi_d \mid V(x) \leq \rho\}$ of $V(x)$ inside ϕ_d as the stability region for the system of Equation (1). Therefore, the origin of the system of Equation (1) is rendered asymptotically stable via the controller $\Phi_s(x)$ in probability if $x(0) = x_0 \in \Omega_\rho$.

In this work, we develop an economic MPC design that takes advantage of the Safeness Index function [2] in its design to achieve probabilistic process operational safety in the following sense:

Definition 3. *Consider the system of Equation (1) with input constraints $u \in U$. If there exists a control law $u = \Phi \in U$ such that the state trajectories of the system for any initial state $x(0) = x_0 \in \mathcal{S}$ satisfy $x(t) \in \mathcal{S}$, $\forall\, t \geq 0$ with the probability p, where $\mathcal{S}$ is a safe operating region in state-space that excludes the unsafe region $\mathcal{D}$, we say that the control law Φ maintains the process state within a safe operating region $\mathcal{S}$ with probability p.*

Remark 1. *In general, the safe operating region $\mathcal{S}$ is characterized as a subset of the stability region (because process operation is safe provided that the system is operated within a closed-loop stability region) for the closed-loop system of Equation (1) to account for the additional safety constraints. Therefore, if there exists a control law $u = \Phi(x) \in U$ that maintains the process state within $\mathcal{S}$ with the probability p, it also maintains the process state within the stability region at least with probability p. This implies that the probability of process operational safety of the system of Equation (1), which we will discuss in the following sections, also gives a lower bound on probabilistic closed-loop stability.*

3. Main Results

In this section, the process Safeness Index and the optimization problem of Safeness Index-based LEMPC designed for the nominal system of Equation (1) with $w(t) \equiv 0$ are first presented. Based on that, the Safeness Index-based LEMPC using multiple level sets of Lyapunov functions is developed for the nominal system of Equation (1) to guarantee recursive feasibility and to guarantee that the closed-loop state does not enter an unsafe operating region $\mathcal{D}$. Subsequently, the stochastic Safeness Index-based LEMPC is developed for the system of Equation (1) to account for the disturbances $w(t)$ with unbounded variation. The stochastic safety and feasibility in probability of the closed-loop system of Equation (1) are finally investigated under the sample-and-hold implementation of the proposed stochastic Safeness Index-based LEMPC.

3.1. Process Safeness Index

In [2], the Safeness Index function $S(x)$ was developed to indicate the level of safety of a given state, through which process operational safety was integrated with process control system design to account for the process operational safety considerations resulting from multivariable interactions or interactions between units. There are various methods of determining the functional form of $S(x)$, for example by utilizing first-principles process models or using systematic safety analysis tools such as HAZOP and fault tree analysis.

Based on the functional form of $S(x)$, the closed-loop state predictions are required to be maintained within a safe region $\mathcal{S}$ (where $S(x)$ is below the threshold on the Safeness Index S_{TH}) by using the Safeness Index-based constraint within the process control design. Additionally, the safety systems (e.g., the alarm, emergency shut-down and relief systems) can be triggered if the threshold S_{TH} is sufficiently exceeded, which implies that the process operation becomes unsafe and further actions are required.

3.2. Safeness Index-Based LEMPC

Safeness Index-based LEMPC optimizes an economic cost function $L_e(\cdot, \cdot)$ and maintains the closed-loop state of the nominal system of Equation (1) with $w(t) \equiv 0$ in a safe operating region by

utilizing the Safeness Index function as a hard constraint within the LEMPC design. Specifically, the formulation of the Safeness Index-based LEMPC is as follows:

$$\max_{u(t)\in ST(\Delta)} \int_{t_k}^{t_k+\tau_P\Delta} L_e(\tilde{x}(\tau), u(\tau))\, d\tau \tag{5a}$$

$$\text{s.t. } \dot{\tilde{x}}(t) = f(\tilde{x}(t)) + g(\tilde{x}(t))u(t) \tag{5b}$$

$$u(t) \in U,\ \forall\ t \in [t_k, t_k + \tau_P\Delta) \tag{5c}$$

$$\tilde{x}(t_k) = x(t_k) \tag{5d}$$

$$V(\tilde{x}(t)) < \rho_e',\ \forall\ t \in [t_k, t_k + \tau_P\Delta) \quad \text{if } x(t_k) \in \Omega^{\mathrm{o}}_{\rho_e'} \tag{5e}$$

$$S(\tilde{x}(t)) \leq S_{TH},\ \forall\ t \in [t_k, t_k + \tau_P\Delta) \quad \text{if } S(x(t_k)) \leq S_{TH} \tag{5f}$$

$$\dot{V}(x(t_k), u(t_k)) \leq \dot{V}(x(t_k), \Phi_n(x(t_k))), \quad \text{if } x(t_k) \in \Omega_{\rho'} \backslash \Omega^{\mathrm{o}}_{\rho_e'} \text{ or } S(x(t_k)) > S_{TH} \tag{5g}$$

where $\tilde{x}$ is the predicted state trajectory, $ST(\Delta)$ is the set of piecewise constant functions with sampling period Δ, τ_P is the number of sampling periods of the prediction horizon and $\dot{V} = L_f V(x) + L_g V(x) u$. $\Phi_n(x)$ is the stabilizing feedback control law designed for the nominal system of Equation (1) with $w(t) \equiv 0$ such that the origin of the system of Equation (1) can be rendered asymptotically stable. Under the controller $\Phi_n(x)$, we first characterize the set $\phi_n := \{x \in \mathbf{R}^n \mid \dot{V} + \kappa V(x) \leq 0, u = \Phi_n(x) \in U, \kappa > 0\}$ and choose the level set $\Omega_{\rho'} := \{x \in \phi_n \mid V(x) \leq \rho'\}$ inside ϕ_n as the stability region. $\Omega_{\rho_e'} := \{x \in \mathbf{R}^n \mid V(x) \leq \rho_e'\}$ where $0 < \rho_e' < \rho'$ is further designed to make the region $\Omega_{\rho'}$ a forward invariant set in the presence of sufficiently small bounded disturbances.

The constraint of Equation (5e) allows the cost function of Equation (5a) to be maximized while keeping the predicted closed-loop state within $\Omega^{\mathrm{o}}_{\rho_e'}$ if $x(t_k) \in \Omega^{\mathrm{o}}_{\rho_e'}$. The safety constraint of Equation (5f) is applied to maintain the predictions of the closed-loop state within the safe operating region $\mathcal{S} := \{x \in \mathbf{R}^n \mid S(x) \leq S_{TH}\}$ if $x(t_k) \in \mathcal{S}$. On the other hand, if $x(t_k) \in \Omega_{\rho'} \backslash \Omega^{\mathrm{o}}_{\rho_e'}$ or $x(t_k)$ is outside of $\mathcal{S}$, the constraint of Equation (5g) is activated to decrease $V(x)$ such that $x(t)$ will move towards the origin within the current sampling period.

Remark 2. *Since the safe operating region $\mathcal{S}$ is not necessarily a forward invariant set based on the formulation of the Safeness Index function, the threshold S_{TH} set on the Safeness Index may define a region that is irregularly shaped, for example the grey region in Figure 1 [2] corresponding to a chemical reactor example similar to the one in the section "Application to a Chemical Process Example" of this manuscript. Therefore, the existence of feasible solutions (i.e., the satisfaction of the constraints of Equation (5)) of the Safeness Index-based LEMPC is not guaranteed in $\mathcal{S}$ due to the constraint of Equation (5f). Additionally, $S(x(t))$ may not even decrease under the constraint of Equation (5g) due to the same reason (that $\mathcal{S}$ is not an invariant set). Considering the above feasibility issue in the formulation of the Safeness Index-based LEMPC, a new Safeness Index-based LEMPC is developed in the following subsection by using multiple Lyapunov functions to characterize the safe operating region $\mathcal{S}$.*

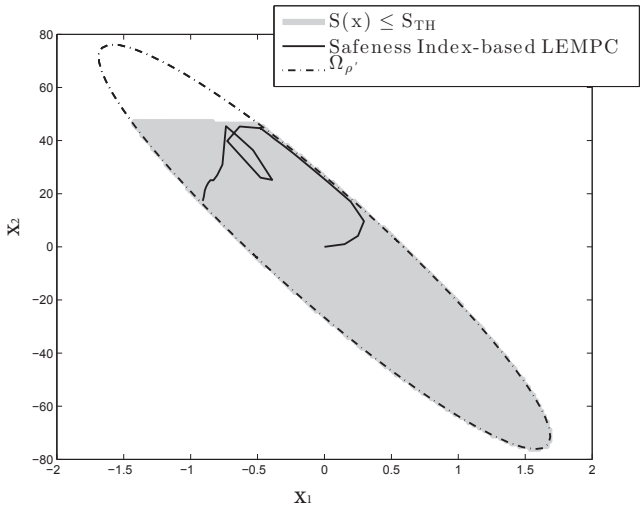

Figure 1. A schematic representing the safe operating region $\mathcal{S}$ (the gray region) with an example closed-loop trajectory under the Safeness Index-based Lyapunov-based economic model predictive control (LEMPC) design of Equation (5) for the initial condition $(0, 0)$.

3.3. Safeness Index-Based LEMPC Using Multiple Level Sets

The improved Safeness Index-based LEMPC for the nominal system of Equation (1) with $w(t) \equiv 0$ is developed utilizing the level sets of two Lyapunov functions V_1 and V_2 to characterize the safe and unsafe operating regions. Throughout this work, we assume that the shape of the stability regions, $\mathcal{D}$, and their intersection are amenable to the treatment in this work, such as the use of only two Lyapunov functions in the LEMPC design and also the types of overlap of the stability regions described. Specifically, as shown in Figure 2, we define two level sets: $\Omega_{\rho'} := \{x \in \phi'_n \mid V_1(x) \leq \rho'\}$ and $\mathcal{U}_{s'} := \{x \in \phi'_n \mid V_2(x) \leq s'\}$ inside $\phi'_n := \{x \in \mathbf{R}^n \mid \dot{V}_i + \kappa V_i(x) \leq 0, i = 1, 2, u = \Phi_n(x) \in U, \kappa > 0\}$, from which the origin of the nominal system of Equation (1) is rendered asymptotically stable.

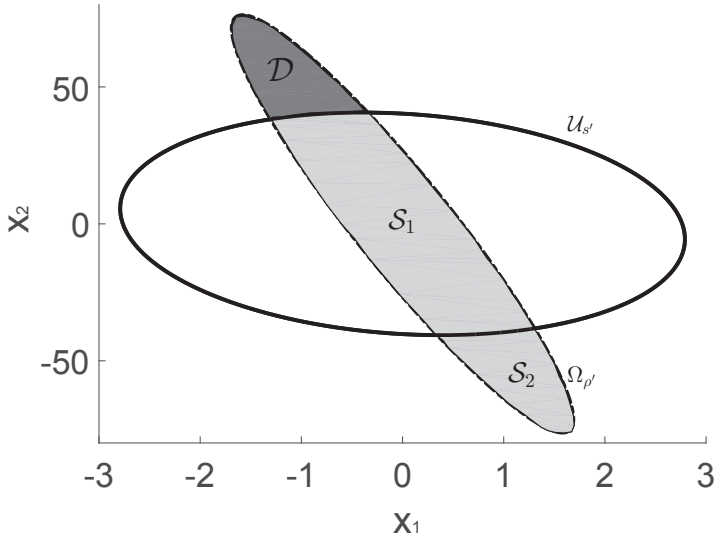

Figure 2. A schematic representing the unsafe region $\mathcal{D}$ (dark gray) and the safe operating region $\mathcal{S} := \mathcal{S}_1 \cup \mathcal{S}_2$ (light gray).

$\Omega_{\rho'}$ represents the stability region as it is in the Safeness Index-based LEMPC of Equation (5), and $\mathcal{U}_{s'}$ is designed to exclude the unsafe region $\mathcal{D}$ where $S(x) > S_{TH}$. Therefore, the safe operating region $\mathcal{S}$ becomes the union of $S_1 := \Omega_{\rho'} \cap \mathcal{U}_{s'}$ and $S_2 := \Omega_{\rho'} \backslash (S_1 \cup \mathcal{D})$ in Figure 2. This new Safeness Index-based LEMPC design is formulated by the following optimization problem:

$$\max_{u \in ST(\Delta)} \int_{t_k}^{t_k+\tau_P\Delta} L_e(\tilde{x}(t), u(t))\, dt \tag{6a}$$

$$\text{s.t. } \dot{\tilde{x}}(t) = f(\tilde{x}(t)) + g(\tilde{x}(t))u(t) \tag{6b}$$

$$\tilde{x}(t_k) = x(t_k) \tag{6c}$$

$$u(t) \in U, \quad \forall\, t \in [t_k, t_k + \tau_P\Delta) \tag{6d}$$

$$V_1(\tilde{x}(t)) < \rho'_e, \quad \text{if } x(t_k) \in \Omega^{\circ}_{\rho'_e}, \quad \forall t \in [t_k, t_k + \tau_P\Delta) \tag{6e}$$

$$V_2(\tilde{x}(t)) < s'_e, \quad \text{if } x(t_k) \in \mathcal{U}^{\circ}_{s'_e}, \quad \forall t \in [t_k, t_k + \tau_P\Delta) \tag{6f}$$

$$\dot{V}_i(x(t_k), u(t_k)) \leq \dot{V}_i(x(t_k), \Phi_n(x(t_k))), i = 1, 2 \quad \text{if } x(t_k) \in \Omega_{\rho'} \backslash \Omega^{\circ}_{\rho'_e}, \text{ or } x(t_k) \in \mathcal{U}_{s'} \backslash \mathcal{U}^{\circ}_{s'_e} \tag{6g}$$

where the notation follows that in Equation (5). $\Omega_{\rho'_e}$ and $\mathcal{U}_{s'_e}$ are again chosen as the level sets inside ϕ'_n to make $\Omega_{\rho'}$ and $\mathcal{U}_{s'}$ forward invariant sets, respectively. In the optimization problem of Equation (6), the objective function of Equation (6a) is the integral of $L_e(\tilde{x}(t), u(t))$ over the prediction horizon. The constraint of Equation (6b) is the nominal system of Equation (1) with $w(t) \equiv 0$ that is used to predict the states of the closed-loop system. Equation (6c) defines the initial condition $\tilde{x}(t_k)$ of the optimization problem determined from a state measurement $x(t_k)$ at $t = t_k$. Equation (6d) represents the input constraints applied over the entire prediction horizon. The constraint of Equation (6e) maintains the predicted states in $\Omega^{\circ}_{\rho'_e}$ when the current state $x(t_k) \in \Omega^{\circ}_{\rho'_e}$. Similarly, the constraint of Equation (6f) maintains the predicted states in $\mathcal{U}^{\circ}_{s'_e}$ when $x(t_k) \in \mathcal{U}^{\circ}_{s'_e}$. The contractive constraint of Equation (6g) is activated to decrease both V_1 and V_2 such that the closed-loop state enters the smaller level sets of V_1 and V_2 (i.e., towards the interior of $\mathcal{S}_1$). Therefore, under the Safeness Index-based LEMPC of Equation (6), if $x(t_k) \in \mathcal{S}_1$, the constraints of Equations (6e)–(6g) maintain the closed-loop state in $\mathcal{S}_1$. If $x(t_k) \in \mathcal{S}_2$, the constraints of Equations (6e) and (6g) are applied to maintain the closed-loop state in $\Omega_{\rho'}$, under which $x(t)$ will stay in $\mathcal{S}_2$ or enter $\mathcal{S}_1$ in some time.

Remark 3. *Based on the Safeness Index function $S(x)$ and its threshold S_{TH}, the level set $\mathcal{U}_{s'}$ of the Lyapunov function V_2 is chosen to exclude the unsafe region $\mathcal{D}$ that is originally in the level set $\Omega_{\rho'}$ of the Lyapunov function V_1 as shown in Figure 2. Since $\mathcal{U}_{s'}$ and $\Omega_{\rho'}$ are both forward invariant sets for the nominal system (or the system with sufficiently small bounded disturbances) of Equation (1) under the controller $\Phi_n(x) \in U$ that satisfies $\dot{V}_i + \kappa V_i(x) \leq 0, i = 1, 2, \kappa > 0$, it follows that under the corresponding constraint of Equation (6g), the overlapping region $\mathcal{S}_1$ is also an invariant set. Therefore, the infeasibility problem caused by the Safeness Index constraint of Equation (5f) is solved by introducing the second level set $\mathcal{U}_{s'}$ into the LEMPC design. For the remaining part of the safe operating region $\mathcal{S}_2$, the constraints of Equations (6e) and (6g) are utilized to ensure that the closed-loop state stays in $\Omega_{\rho'}$ all the time, which is similar to closed-loop stability under the traditional LEMPC [4]. Since the sampling period Δ has to be sufficiently small in the sample-and-hold implementation of the Safeness Index-based LEMPC of Equation (6), we can utilize a sufficiently small Δ such that $x(t_{k+1})$ is unable to jump into $\mathcal{D}$ within one sampling period if $x(t_k) \in \mathcal{S}_2$. This implies that at the next sampling time, the state $x(t_{k+1})$ either stays in $\mathcal{S}_2$ or enters $\mathcal{S}_1$ via the boundary between $\mathcal{S}_1$ and $\mathcal{S}_2$. In both cases, it is considered that the state is maintained in the safe operating region according to Definition 3.*

Remark 4. *Besides the above development of Safeness Index-based LEMPC using multiple Lyapunov functions, there are also other methods that can guarantee the feasibility of the Safeness Index-based constraint in the LEMPC design. For example, in the optimization problem of Equation (5), we can choose a more conservative level set of $V(x)$ (i.e., a small level set inside $\Omega_{\rho'}$ that excludes $\mathcal{D}$) as the safe operating region. However, if the unsafe region characterized by the Safeness Index function is a set of points inside the stability region and is difficult to exclude by a single level set like $\mathcal{U}_{s'}$, we may want to use control Lyapunov barrier functions to design the constraints that account for the unsafe region in state-space [15] and overcome the infeasibility problem.*

3.4. Stochastic Safeness Index-Based LEMPC

Inspired by the Safeness Index-based LEMPC design of Equation (6), the stochastic Safeness Index-based LEMPC design is given by the following optimization problem:

$$\max_{u\in ST(\Delta)} \int_{t_k}^{t_k+\tau_P\Delta} L_e(\tilde{x}(t), u(t))\, dt \tag{7a}$$

$$\text{s.t. } \dot{\tilde{x}}(t) = f(\tilde{x}(t)) + g(\tilde{x}(t))u(t) \tag{7b}$$

$$\tilde{x}(t_k) = x(t_k) \tag{7c}$$

$$u(t) \in U, \quad \forall\, t \in [t_k, t_k + \tau_P\Delta) \tag{7d}$$

$$V_1(\tilde{x}(t)) < \rho_e, \quad \text{if } x(t_k) \in \Omega^{\circ}_{\rho_e}, \quad \forall t \in [t_k, t_k + \tau_P\Delta) \tag{7e}$$

$$V_2(\tilde{x}(t)) < s_e, \quad \text{if } x(t_k) \in \mathcal{U}^{\circ}_{s_e}, \quad \forall t \in [t_k, t_k + \tau_P\Delta) \tag{7f}$$

$$\mathcal{L}V_i(x(t_k), u(t_k)) \leq \mathcal{L}V_i(x(t_k), \Phi_s(x(t_k))), i = 1, 2 \quad \text{if } x(t_k) \in \Omega_\rho \backslash \Omega^{\circ}_{\rho_e}, \text{ or } x(t_k) \in \mathcal{U}_s \backslash \mathcal{U}^{\circ}_{s_e} \tag{7g}$$

where the notation follows that in Equation (6) except using ρ, ρ_e, s, s_e, $\Phi_s(x)$ and $\mathcal{L}V$ to replace ρ', ρ'_e, s', s'_e, $\Phi_n(x)$ and $\dot{V}$, respectively. For the system of Equation (1) with multiple Lyapunov functions, ϕ_d is characterized as: $\phi_d = \{x \in \mathbf{R}^n \mid \mathcal{L}V_i + \kappa V_i(x) \leq 0, i = 1, 2, u = \Phi_s(x) \in U, \kappa > 0\}$. Ω_ρ, Ω_{ρ_e}, $\mathcal{U}_s$ and $\mathcal{U}_{s_e}$ are level sets of V_1 and V_2 inside ϕ_d, where $0 < \rho_e < \rho$ and $0 < s_e < s$. Similar to the LEMPC designs of Equations (5) and (6), the optimal input trajectory determined by the optimization problem of the stochastic Safeness Index-based LEMPC is denoted by $u^*(t)$, which is calculated over the entire prediction horizon $t \in [t_k,\, t_k + \tau_P\Delta)$. The control action computed for the first sampling period of the prediction horizon $u^*(t_k)$ is sent to the actuators to be applied over the sampling period, and the optimization problem of Equation (7) is re-solved at the next sampling time.

The constraint of Equation (7e) maintains the predicted state in $\Omega^{\circ}_{\rho_e}$ when the current state $x(t_k) \in \Omega^{\circ}_{\rho_e}$ and the constraint of Equation (7f) maintains the predicted state in $\mathcal{U}^{\circ}_{s_e}$ when the current state $x(t_k) \in \mathcal{U}^{\circ}_{s_e}$. However, if $x(t_k) \in \Omega_\rho \backslash \Omega^{\circ}_{\rho_e}$ or $x(t_k) \in \mathcal{U}_s \backslash \mathcal{U}^{\circ}_{s_e}$, the constraint of Equation (7g) is activated to decrease $V_1(x)$ and $V_2(x)$ such that it is possible that $x(t)$ moves back to $\Omega^{\circ}_{\rho_e} \cap \mathcal{U}^{\circ}_{s_e}$.

Since there exists a disturbance $w(t)$ with unbounded variation $dw(t)$ in the system of Equation (1), process operational safety (i.e., the closed-loop state is bounded in the safe operating region $\mathcal{S}$) can only be ensured in probability. Therefore, in the following sections, we will establish the probabilities of process operational safety of the system of Equation (1) under the stochastic Safeness Index-based LEMPC of Equation (7).

3.5. Sample-And-Hold Implementation

We first investigate the impact of the sample-and-hold implementation of Equation (7) on the stability of the closed-loop system of Equation (1) following similar arguments to those in [9,11]. Specifically, the probabilities of the sets Ω_ρ and $\mathcal{U}_s$ remaining invariant under the sample-and-hold

implementation of the Safeness Index-based LEMPC of Equation (7) with a sampling period Δ are given as follows.

Theorem 1. *Consider the system of Equation (1) with Ω_ρ and $\mathcal{U}_s$ inside ϕ_d under the control actions u computed by the LEMPC of Equation (7). Let $u(t) = u(t_k), \forall t \in [t_k, t_k + \Delta)$. Then, given any probability $\lambda \in (0, 1]$, there exist positive real numbers $\rho_s < \rho_e < \rho$ and $\rho_s < s_e < s$ where Ω_{ρ_s} and $\mathcal{U}_{\rho_s}$ are level sets of V_1 and V_2, respectively, around the origin where $\mathcal{L}V_i$, $i = 1, 2$ are not required to remain negative for the nominal system of Equation (1) under the sample-and-hold implementation of $u(t)$, and there also exists a sampling period $\Delta^* := \Delta^*(\lambda)$, such that if $\Delta \in (0, \Delta^*]$, then:*

$$\mathbf{P}(\sup_{t\in[0,\Delta]} V_1(x(t)) < \rho) \geq 1 - \lambda, \ \forall x(0) \in \Omega^o_{\rho_e} \tag{8}$$

$$\mathbf{P}(\sup_{t\in[0,\Delta]} V_2(x(t)) < s) \geq 1 - \lambda, \ \forall x(0) \in \mathcal{U}^o_{s_e} \tag{9}$$

$$\begin{aligned} &\mathbf{P}(\sup_{t\in[0,\Delta]} \mathcal{L}V_i(x(t)) < -\epsilon < 0) \geq 1 - \lambda, \ i = 1, 2, \\ &\forall x(0) \in (\Omega_\rho \cup \mathcal{U}_s) \backslash (\Omega^o_{\rho_s} \cap \mathcal{U}^o_{\rho_s}) \end{aligned} \tag{10}$$

Proof. Let $A_B := \{w : \sup_{t\in[0,\Delta^*]} |w(t)| \leq B\}$. Using the results for standard Brownian motion [16], given any probability $\lambda \in (0, 1]$, there exists a sufficiently small B, s.t. $P(A_B) = 1 - \lambda$. For each realization $x_w(t)$ with $x(0) \in \Omega_\rho \cup \mathcal{U}_s$ and $w \in A_B$, there almost surely exists a positive real number k_1, s.t. $\sup_{t\in[0,\Delta^*]} |x_w(t) - x(0)| \leq k_1(\Delta^*)^r$, where $r < 1/2$, according to the local Hölder continuity. Therefore, the probability of the event $A_W := \{w : \sup_{t\in[0,\Delta^*]} |x(t) - x(0)| \leq k_1(\Delta^*)^r\}$ is:

$$\mathbf{P}(A_W) \geq 1 - \lambda \tag{11}$$

We first prove that the probabilities of Equations (8) and (9) hold for the first sampling period. It should be noted that the probabilities of Equations (8)–(10) can be generalized to any sampling period $t \in [t_k, t_k + \Delta]$ with the measurement of $x(t_k)$ playing the role of $x(0)$ in Equations (8)–(10).

Since $V_i(x)$, $i = 1, 2$ satisfies the local Lipschitz condition, there exist positive real numbers k_{2i}, $i = 1, 2$, such that $|V_i(x(t)) - V_i(x(0))| \leq k_{2i}|x(t) - x(0)|$, $i = 1, 2$. Therefore, for all $w \in A_W$, if $\Delta^* < \Delta_1 = (\frac{\rho-\rho_e}{k_{21}k_1})^{(\frac{1}{r})}$, it follows that $|V_1(x_w(t)) - V_1(x(0))| < \rho - \rho_e, \forall t \leq \Delta^*$. Furthermore, $\forall x(0) \in \Omega^o_{\rho_e}$, it is obtained that $V_1(x_w(t)) < \rho$, $\forall t \leq \Delta^*$ since $-(\rho - \rho_e) < V_1(x(t)) - V_1(x(0)) < \rho - \rho_e$ and $\sup_{x(0)\in\Omega^o_{\rho_e}} V_1(x(0)) = \rho_e$. Therefore, if $x(0) \in \Omega^o_{\rho_e}$, the probability of $x(t)$ staying inside Ω_ρ is $\mathbf{P}(\sup_{t\in[0,\Delta^*]} V_1(x(t)) < \rho) \geq 1 - \lambda$. Similarly, if $\Delta^* < \Delta_2 = (\frac{s-s_e}{k_{22}k_1})^{(\frac{1}{r})}$, for any $x(0) \in \mathcal{U}^o_{s_e}$, the probability of $x(t)$ staying inside $\mathcal{U}_s$ is $\mathbf{P}(\sup_{t\in[0,\Delta^*]} V_2(x(t)) < s) \geq 1 - \lambda$.

We now prove the probability of Equation (10) by using the equation $\mathcal{L}V_i(x(t)) = \mathcal{L}V_i(x(0)) + (\mathcal{L}V_i(x(t)) - \mathcal{L}V_i(x(0)))$, $\forall t \in [0, \Delta^*]$, $i = 1, 2$. It is shown that there exists a positive real number ϵ such that $\mathcal{L}V_i(x(t)) < -\epsilon$ holds $\forall x(0) \in (\Omega_\rho \cup \mathcal{U}_s) \backslash (\Omega^o_{\rho_s} \cap \mathcal{U}^o_{\rho_s})$ for the nominal system of Equation (1) based on the definition of the value of $\mathcal{L}V_i$ in ϕ_d. However, $\mathcal{L}V_i(x(t)) < -\epsilon$ only holds in probability for the system in the presence of the disturbances $w(t)$. Based on the local Lipschitz conditions of $L_fV_i(x)$, $L_gV_i(x)$ and $h(x(t))^T \frac{\partial^2 V_i(x(t))}{\partial x^2} h(x(t))$, there exist positive real numbers k_3, k_4, k_5, such that $|L_fV_i(x(t)) - L_fV_i(x(0))| \leq k_3|x(t) - x(0)|$, $|L_gV_i(x(t)) - L_gV_i(x(0))| \leq k_4|x(t) - x(0)|$, $|\frac{1}{2}Tr\{h(x(t))^T \frac{\partial^2 V_i(x(t))}{\partial x^2} h(x(t))\} - \frac{1}{2}Tr\{h(x(0))^T \frac{\partial^2 V_i(x(0))}{\partial x^2} h(x(0))\}| \leq k_5|x(t) - x(0)|$, $i = 1, 2$.

Let $0 < \epsilon < \kappa\rho_s$ and $\Delta^* < \Delta_3 = (\frac{\kappa\rho_s - \epsilon}{k_1(k_3+k_4+k_5)})^{(\frac{1}{r})}$. It follows from $\mathcal{L}V_i(x(t)) \leq \mathcal{L}V_i(x(0)) + |\mathcal{L}V_i(x(t)) - \mathcal{L}V_i(x(0))| < \mathcal{L}V_i(x(0)) + \kappa\rho_s - \epsilon$ (which follows from the application of the Lipschitz properties of the components of $\mathcal{L}V_i$ with $\Delta^* < \Delta_3$) and the fact that $x(0) \in (\Omega_\rho \cup \mathcal{U}_s) \backslash (\Omega^o_{\rho_s} \cap \mathcal{U}^o_{\rho_s})$ and $\mathcal{L}V_i(x_0) < -\kappa V_i(x(0))$, that $\forall w \in A_W$, $\mathcal{L}V_i(x_w(t)) < -\epsilon < 0$, $\forall t \leq \Delta^*$, $i = 1, 2$ holds. Therefore, by choosing the sampling period $\Delta \in (0, \Delta^*]$, given any initial condition $x(0) \in (\Omega_\rho \cup \mathcal{U}_s) \backslash (\Omega^o_{\rho_s} \cap \mathcal{U}^o_{\rho_s})$,

the probability that $\mathcal{L}V_i(x(t)) < -\epsilon$ is as follows: $\mathbf{P}(\sup_{t\in[0,\Delta^*]} \mathcal{L}V_i(x(t)) < -\epsilon,\ i = 1,2) \geq 1-\lambda$. Finally, let $\Delta^* \leq \min\{\Delta_1, \Delta_2, \Delta_3\}$, and the probabilities of Equations (8)–(10) are all satisfied for $\Delta \in (0, \Delta^*]$. □

3.6. Stability in Probability

Based on the results from the above section, the probabilistic process operational safety of the closed-loop system of Equation (1) under the Safeness Index-based LEMPC of Equation (7) applied in a sample-and-hold fashion is established by the following theorem.

Theorem 2. *Consider the system of Equation (1) under the stochastic Safeness Index-based LEMPC of Equation (7) applied in a sample-and-hold implementation (i.e., $u(t) = u(i\Delta),\ \forall\ i\Delta \leq t < (i+1)\Delta$, $i = 0, 1, 2, ...$). Then, given $\rho_e \in (0, \rho)$, $s_e \in (0, s)$ and probability $\lambda \in (0, 1]$, there exist a sampling time $\Delta \in (0, \Delta^*(\lambda)]$ and probabilities $\beta, \beta', \gamma, \gamma' \in [0, 1]$:*

$$\frac{\sup_{x\in\partial\Omega_{\rho_e}} V_1(x)}{\inf_{x\in\mathbf{R}^n\backslash\Omega_\rho} V_1(x)} \leq \beta \tag{12a}$$

$$\frac{\sup_{x\in\partial\mathcal{U}_{s_e}} V_2(x)}{\inf_{x\in\mathbf{R}^n\backslash\mathcal{U}_s} V_2(x)} \leq \beta' \tag{12b}$$

$$\max\{\frac{V_1(x(0))}{\rho}, \beta\} \leq \gamma \tag{12c}$$

$$\max\{\frac{V_2(x(0))}{s}, \beta'\} \leq \gamma' \tag{12d}$$

such that the following probabilities hold:

$$\begin{aligned}&\mathbf{P}(\sup_{t\in[0,\Delta)} V_1(x(t)) < \rho,\ \sup_{t\in[0,\Delta)} V_2(x(t)) < s)\\ &\quad\geq (1-\beta)(1-\beta')(1-\lambda),\quad \forall x(0) \in \mathcal{S}_{1e}\end{aligned} \tag{13}$$

$$\begin{aligned}&\mathbf{P}(\sup_{t\in[0,\Delta)} V_1(x(t)) < \rho)\\ &\quad\geq (1-\beta)(1-\lambda),\quad \forall x(0) \in \mathcal{S}_{2e}\end{aligned} \tag{14}$$

$$\begin{aligned}&\mathbf{P}(\tau_{\mathbf{R}^n\backslash\mathcal{S}_{1e}}(\Delta) \leq \tau_{\mathcal{S}_1}(\Delta))\\ &\quad\geq (1-\gamma)(1-\gamma')(1-\lambda),\quad \forall x(0) \in \mathcal{S}_1\backslash\mathcal{S}_{1e}^o\end{aligned} \tag{15}$$

where $\mathcal{S}_e := \mathcal{S}_{1e} \cup \mathcal{S}_{2e}$ is a subset of $\mathcal{S}$ that subtracts the risk margins $\rho - \rho_e$ and $s - s_e$. The relationship among the sets $\mathcal{S}_{1e} := \Omega_{\rho_e} \cap \mathcal{U}_{s_e}$ and $\mathcal{S}_{2e} := \mathcal{S}_e\backslash\mathcal{S}_{1e}$ and the unsafe region $\mathcal{D}$ are shown in Figure 3.

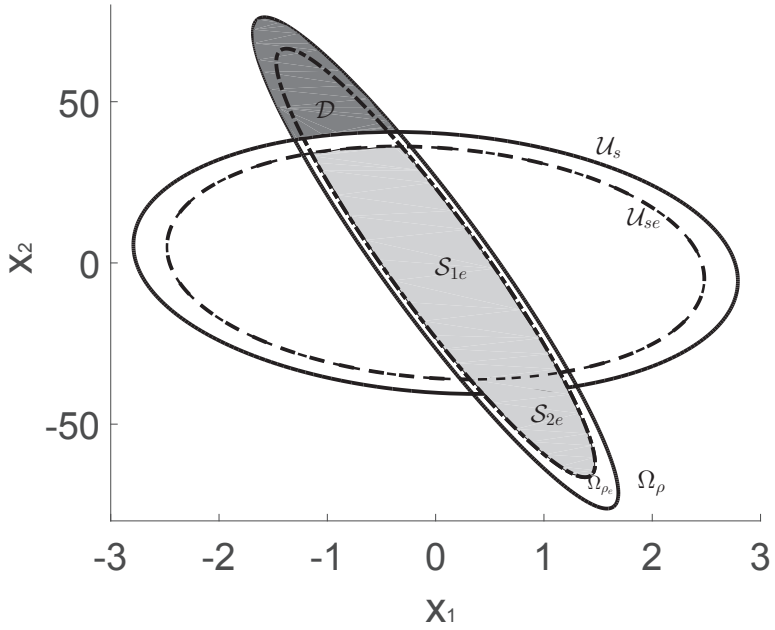

Figure 3. A schematic representing the unsafe region $\mathcal{D}$ (dark gray) and the region $\mathcal{S}_e := \mathcal{S}_{1e} \cup \mathcal{S}_{2e}$ (light gray), which is the safe operating region $\mathcal{S}$ subtracting the risk margins $\rho - \rho_e$ and $s - s_e$.

Proof. The proof consists of three parts. We first show that under the Safeness Index-based LEMPC of Equation (7), any state trajectory initiated from $x(0) \in \mathcal{S}_{1e}$ has the probability defined by Equation (13) of staying in $\mathcal{S}_1 := \Omega_\rho \cap \mathcal{U}_s$. However, if $x(0) \in \mathcal{S}_{2e}$, we prove that under the Safeness Index-based LEMPC of Equation (7), there exists the probability of Equation (14) for the state of the closed-loop system to stay in Ω_ρ and with a sufficiently small Δ to stay in the part of Ω_ρ that excludes $\mathcal{D}$. Finally, if $x(0)$ is inside $\mathcal{S}_1 \backslash \mathcal{S}_{1e}^o$, we can show that the closed-loop state trajectory reaches the boundary of $\mathcal{S}_{1e}$ first before it leaves $\mathcal{S}_1$ (implying it does not enter $\mathcal{D}$) with the probability of Equation (15). However, if $x(0) \in \Omega_\rho \backslash \Omega_{\rho_e}^o$ and $x(0) \notin (\mathcal{U}_s \cup \mathcal{D})$ (i.e., the white risk margin around $\mathcal{S}_{2e}$ in Figure 3), we show that it does not enter $\mathcal{D}$, $\forall t \in [0, \Delta)$ in probability, as well. Additionally, for the sake of simplicity, we denote the probabilities and expectations conditional on the event of A_W given in the section "Sample-And-Hold Implementation" as $\mathbf{P}^*(\cdot)$ and $\mathbf{E}^*(\cdot)$.

Part 1: To show that Equation (13) holds for all $x(0) \in \mathcal{S}_{1e}$, we consider both the case that $x(0) \in S_{1e}^o$ and that $x(0) \in \partial S_{1e}$. The former case is handled by Equations (8) and (9). Specifically, if $x(0) \in S_{1e}^o$, then both $x(0) \in \Omega_{\rho_e}^o$ and also $x(0) \in \mathcal{U}_{s_e}^o$. Then, $\mathbf{P}(\sup_{t\in[0,\Delta)} V_1(x(t)) < \rho, \sup_{t\in[0,\Delta)} V_2(x(t)) < s) \geq 1 - \lambda$ (Equations (8) and (9) for $\Delta^* \leq \min\{\Delta_1, \Delta_2\}$). Since $(1-\lambda) \geq (1-\beta)(1-\beta')(1-\lambda)$ for $\beta \in [0,1]$, $\beta' \in [0,1]$, Equation (13) holds when $x(0) \in S_{1e}^o$. When $x(0) \in \partial\mathcal{S}_{1e}$, Equation (13) is also satisfied. To show this, we first assume $x(0) \in \partial\Omega_{\rho_e}$ and prove that the probability of $x(t)$ staying in Ω_ρ within one sampling period conditioned on the event of A_W is $(1-\beta)$. When $x(0) \in \partial\Omega_{\rho_e}$, Equation (7g) will be utilized in the LEMPC of Equation (7). Under the constraint of Equation (7g), the optimization problem of Equation (7) is solved such that $\mathcal{L}V_1$ is forced to be negative for any $x(t_k) \in \Omega_\rho \backslash \Omega_{\rho_e}^o$, which implies that Equation (10) holds (i.e., $\mathcal{L}V_1 < -\epsilon$ for $t \in [0, \Delta]$ with the probability of the event A_W). Using Dynkin's formula [17], the following equation can be derived:

$$\begin{aligned} &\mathbf{E}^*(V_1(x(\tau_{\Omega_\rho \backslash \Omega_{\rho_e}^o}(t)))) \\ &\quad = V_1(x(0)) + \mathbf{E}^*\Big(\int_0^{\tau_{\Omega_\rho \backslash \Omega_{\rho_e}^o}(t)} \mathcal{L}V_1(x(s))ds\Big) \end{aligned} \tag{16}$$

The following probability is derived using similar arguments as in [11], for all $x(0) \in \partial\Omega_{\rho_e}$:

$$\begin{aligned} &\mathbf{P}^*(V_1(x(t)) \geq \rho, \text{ for some } t \in [0, \Delta)) \\ &\leq \frac{V_1(x(0))}{\inf_{x \in \mathbf{R}^n \backslash \Omega_\rho} V_1(x)} \end{aligned} \tag{17}$$

Bounding Equation (17) with Equation (12a) and taking the complementary events, the following probability is obtained:

$$\inf_{x(0) \in \partial\Omega_{\rho_e}} \mathbf{P}^*(V_1(x(t)) < \rho, \forall t \in [0, \Delta)) \geq (1 - \beta) \tag{18}$$

Using the same steps as performed above, we can prove that $\forall x(0) \in \partial\mathcal{U}_{s_e}$, the probability of $x(t)$ staying in $\mathcal{U}_s$ within one sampling period conditioned on the event of A_W is as follows:

$$\inf_{x(0) \in \partial\mathcal{U}_{s_e}} \mathbf{P}^*(V_2(x(t)) < s, \forall t \in [0, \Delta)) \geq (1 - \beta') \tag{19}$$

Since the set of initial conditions $x(0) \in \mathcal{S}_{1e}$ is the intersection of Ω_{ρ_e} and $\mathcal{U}_{s_e}$, by combining the probabilities of Equations (18) and (19) together and using Equation (10), the probability of Equation (13) is obtained via the definition of conditional probability.

Part 2: If $x(0) \in S_{2e} \subset \Omega_{\rho_e}$, then either $x(0) \in \Omega^o_{\rho_e}$ or $x(0) \in \partial\Omega_{\rho_e}$. If $x(0) \in S_{2e}$ and $\Omega^o_{\rho_e}$, then Equation (8) holds and $\mathbf{P}(\sup_{t \in [0,\Delta)} V_1(x(t)) < \rho) \geq 1 - \lambda \geq (1 - \beta)(1 - \lambda)$ for $\beta \in [0, 1]$, and Equation (14) therefore holds. If instead $x(0) \in S_{2e}$ and $\partial\Omega_{\rho_e}$, then the results of Part 1 indicate that Equation (18) holds. Applying the definition of conditional probability, this also gives that Equation (14) holds. Moreover, we show that $x(t)$ is maintained inside the safe operating region $\mathcal{S}$ within one sampling period with the probability of Equation (14) (i.e., $\forall t \in [0, \Delta)$, $x(t)$ will not jump into $\mathcal{D}$ in probability). It is shown in the section "Sample-And-Hold Implementation" that $\forall t \in [0, \Delta)$, the change of $V_i(x)$ is limited (i.e., $|V_1(x(t)) - V_1(x(0))| < k_1 k_{21} \Delta^*, \forall t \leq \Delta^*$ and $|V_2(x(t)) - V_2(x(0))| < k_1 k_{22} \Delta^*, \forall t \leq \Delta^*$) with a sufficiently small sampling period Δ^* (maybe smaller than the one derived by $\Delta^* \leq \min\{\Delta_1, \Delta_2, \Delta_3\}$). Therefore, if $x(0) \in \mathcal{S}_{2e} \subset \Omega_{\rho_e}$, $x(t)$ cannot move across the entire level set $\mathcal{U}_s$ and jump into $\mathcal{D}$ within a sufficiently small Δ with the probability $(1 - \lambda)$. Instead, the closed-loop state at the next sampling time either stays in $\mathcal{S}_{2e}$ or moves into $\mathcal{S}_{1e}$ in probability. If $x(t)$ enters $\mathcal{S}_{1e}$, the probability of Equation (13) will be used to estimate the probability of closed-loop process operational safety thereafter. Because $(1 - \lambda) \geq (1 - \beta)(1 - \lambda)$, for $\beta, \lambda \in (0, 1]$, Equation (14) establishes the probability of $x(t)$ staying in the safe operating region $\mathcal{S}$ within one sampling period $\forall x(0) \in \mathcal{S}_{2e}$.

Part 3: If $x(0) \in \mathcal{S}_1 \backslash \mathcal{S}^o_{1e}$, we show that it is possible that the closed-loop state trajectory hits the boundary of $\mathcal{S}^o_{1e}$ before it hits the boundary of $\mathcal{S}_1$. If both hitting times $\tau_{\mathbf{R}^n \backslash \mathcal{S}_{1e}}(\Delta)$ and $\tau_{\mathcal{S}_1}(\Delta)$ are longer than a sampling period Δ, Equation (15) is trivially satisfied. However, if one of them or both occur within one sampling period, we show that the probability of Equation (15) holds by first showing that the extreme case that $x(0) \in (\Omega_\rho \backslash \Omega^o_{\rho_e}) \cap (\mathcal{U}_s \backslash \mathcal{U}^o_{s_e})$ (which are the corners where the risk margins $\rho - \rho_e$ and $s - s_e$ overlap in Figure 3) satisfies Equation (15). We first show that the probability of the event $A_T := \{\tau_{\mathbf{R}^n \backslash \Omega^o_{\rho_e}} > \tau_{\Omega_\rho}\}$ can be given as follows $\forall x(0) \in \Omega_\rho \backslash \Omega^o_{\rho_e}$:

$$\mathbf{P}^*(\tau_{\mathbf{R}^n \backslash \Omega^o_{\rho_e}} > \tau_{\Omega_\rho}) \leq \mathbf{P}^*(\frac{V_1(x(\tau_{\Omega_\rho \backslash \Omega^o_{\rho_e}}))}{\rho} \geq 1) \leq \frac{V_1(x(0))}{\rho} \tag{20}$$

The event A_T indicates that the state of the closed-loop system of Equation (1) reaches the boundary of Ω_ρ before it reaches the boundary of Ω_{ρ_e}. The probability of Equation (20) is determined via Equation (17) and the fact that the event $\{\tau_{\mathbf{R}^n \backslash \Omega^o_{\rho_e}} > \tau_{\Omega_\rho}\}$ belongs to the event $\{\frac{V_1(x(\tau_{\Omega_\rho \backslash \Omega^o_{\rho_e}}))}{\rho} \geq 1\}$.

Assuming $x(0) \in \partial\Omega_{\rho_c}$, where $\Omega_{\rho_c} := \{x \in \phi_d \mid V_1(x) \leq \rho_c\}$ and $\rho_c \in [\rho_e, \rho]$, the following probability is derived by bounding Equation (20) by Equation (12c):

$$\sup_{x(0)\in\Omega_{\rho_c}\backslash\Omega^o_{\rho_e}} \mathbf{P}^*(\tau_{\mathbf{R}^n\backslash\Omega^o_{\rho_e}} > \tau_{\Omega_\rho}) \leq \gamma \tag{21}$$

Using the same steps as performed above, we can prove that $\forall x(0) \in \mathcal{U}_s\backslash\mathcal{U}^o_{s_e}$, the probabilities similar to Equations (20) and (21) are derived as follows:

$$\mathbf{P}^*(\tau_{\mathbf{R}^n\backslash\mathcal{U}^o_s} > \tau_{\mathcal{U}_s}) \leq \frac{V_2(x(0))}{s} \tag{22a}$$

$$\sup_{x(0)\in\mathcal{U}_{s_c}\backslash\mathcal{U}^o_{s_e}} \mathbf{P}^*(\tau_{\mathbf{R}^n\backslash\mathcal{U}^o_{s_e}} > \tau_{\mathcal{U}_s}) \leq \gamma' \tag{22b}$$

where $\mathcal{U}_{s_c} := \{x \in \phi_d \mid V_2(x) \leq s_c\}$ and $s_c \in [s_e, s]$. Hence, the probability $\mathbf{P}(\tau_{\mathbf{R}^n\backslash\mathcal{S}_{1e}}(\Delta) \leq \tau_{\mathcal{S}_1}(\Delta))$ (i.e., Equation (15)) for the case where $x(0) \in (\Omega_\rho\backslash\Omega^o_{\rho_e}) \cap (\mathcal{U}_s\backslash\mathcal{U}^o_{s_e}) \subset \mathcal{S}_1\backslash\mathcal{S}^o_{1e}$ is obtained by taking the complementary event of Equations (21) and (22b) and using the definition of conditional probability. We now address the other two possibilities for $x(0) \in \mathcal{S}_1\backslash\mathcal{S}^o_{1e}$ besides $x(0) \in (\Omega_\rho\backslash\Omega^o_{\rho_e}) \cap (\mathcal{U}_s\backslash\mathcal{U}^o_{s_e})$, which are: (1) $x(0) \in (\Omega_\rho\backslash\Omega^o_{\rho_e}) \cap \mathcal{U}^o_{s_e}$ and (2) $x(0) \in (\mathcal{U}_s\backslash\mathcal{U}^o_{s_e}) \cap \Omega^o_{\rho_e}$. Consider the case where $x(0) \in (\Omega_\rho\backslash\Omega^o_{\rho_e}) \cap \mathcal{U}^o_{s_e}$. If $x(t) \in \mathcal{U}^o_{s_e}$, $\forall t \in [0, \Delta)$, then $\mathbf{P}^*(\tau_{\mathbf{R}^n\backslash\mathcal{S}_{1e}}(\Delta) \leq \tau_{\mathcal{S}_1}(\Delta))$=$\mathbf{P}^*(\tau_{\mathbf{R}^n\backslash\Omega^o_{\rho_e}}(\Delta) \leq \tau_{\Omega_\rho}(\Delta))$. If $x(t)$ enters $\mathcal{U}_s\backslash\mathcal{U}^o_{s_e}$ before it leaves $\Omega_\rho\backslash\Omega^o_{\rho_e}$, for some $t \in [0, \Delta)$, then for sure it holds that $\tau_{\mathbf{R}^n\backslash\mathcal{S}_{1e}}(\Delta) < \tau_{\mathcal{S}_1}(\Delta)$ because the closed-loop state trajectory crosses the boundary of $\mathcal{S}_{1e}$ first. Therefore, Equation (15) holds for both cases. The same analysis can be performed for the case where $x(0) \in (\mathcal{U}_s\backslash\mathcal{U}^o_{s_e}) \cap \Omega^o_{\rho_e}$. However, if $x(0) \in \Omega_\rho\backslash\Omega^o_{\rho_e}$ and $x(0) \notin (\mathcal{U}_s \cup \mathcal{D})$, it is readily shown that Equation (21) holds due to the fact that $x(0) \in \Omega_\rho\backslash\Omega^o_{\rho_e}$. Additionally, since it is demonstrated in *Part* 2 that the change of $V_i(x)$ within one sampling period is limited in probability, it follows that $\forall x(0) \in \Omega_\rho\backslash\Omega^o_{\rho_e}$ and $x(0) \notin (\mathcal{U}_s \cup \mathcal{D})$, $x(t)$ does not enter $\mathcal{D}$ in one sampling period with the probability of $1 - \lambda$, which implies that the closed-loop state either stays in $\mathcal{S}_2$ or moves into $\mathcal{S}_1$ in probability. □

Remark 5. *The Safeness Index-based LEMPC of Equation (7) is unable to ensure process operational safety for the closed-loop system of Equation (1) because of stochastic disturbances with unbounded variation. Additionally, in order to achieve process operational safety with higher probability, we should characterize the safe operating region $\mathcal{S}$ well and design large enough risk margins (i.e., $\rho - \rho_e$ and $s - s_e$) to avoid frequent activations of backup safety systems. Specifically, in Theorem 2, it is shown that as ρ_e and s_e decrease, the probabilities of Equations (13)–(15) become larger, which implies that if we want to improve process operational safety, the Safeness Index-based LEMPC design of Equation (7) should be designed with more conservatism (i.e., choosing smaller ρ_e and s_e). However, an operating region with smaller ρ_e and s_e in turn leads to less economic benefits, which is undesired for the Safeness Index-based LEMPC of Equation (7). Therefore, the uncertain process operational safety caused by stochastic disturbances with unbounded variation is essentially a trade-off between economic benefits and probabilistic process operational safety (i.e., in practice, we will choose a conservative operating region to make the process sufficiently safe with respect to the unbounded disturbances, especially considering the other safety systems online and the risks involved, while also optimizing process economics).*

3.7. Feasibility in Probability

Recursive feasibility for the nominal system of Equation (1) with $w(t) \equiv 0$ under the Safeness Index-based LEMPC of Equation (6) is guaranteed since there always exists a solution (e.g., the Lyapunov-based controller $\Phi_n(x)$ in sample-and-hold) that satisfies all the constraints of Equation (6). Now, consider the system of Equation (1) that has disturbance $w(t)$ with unbounded variation. Recursive feasibility under the stochastic Safeness Index-based LEMPC of Equation (7) can only be guaranteed in probability over the operation period $t \in [0, \tau_N\Delta)$. The probability is established as follows, from which it is shown that the probabilistic bounds on recursive feasibility for the remainder

of the entire time of operation decrease as the operation period becomes longer (however, this does not necessarily mean the closed-loop system will not remain recursively feasible because at every sampling time, the remaining time of operation decreases and therefore the probability that the LEMPC will remain recursively feasible for the remaining time of operation increases at the next sampling time if the closed-loop state was maintained within $\mathcal{S}$ throughout the prior sampling period).

Theorem 3. *Consider the system of Equation (1) under the stochastic Safeness Index-based LEMPC of Equation (7) applied in a sample-and-hold fashion. Then, if $x(0) \in \mathcal{S}$, let $V_1(x(t+i\Delta)) = \rho_i < \rho$, $V_2(x(t+i\Delta)) = s_i < s$, $i = 0, 1, ..., \tau_N - 1$, and let A_F represent the event that the optimization problem of Equation (7) is solved with the satisfaction of recursive feasibility for time $t \in [0, \tau_N\Delta)$. The probability of A_F can be calculated as follows:*

$$\mathbf{P}(A_F) \geq (1-\lambda)^{\tau_N} \prod_{i=0,1,...,\tau_N-1} (1-\beta_i)(1-\beta_i') \tag{23}$$

where β_i and β_i' are given as follows:

$$\beta_i = \max\{\beta, \frac{\sup_{x\in\partial\Omega_{\rho_i}} V_1(x)}{\inf_{x\in\mathbf{R}^n\setminus\Omega_\rho} V_1(x)}\} \tag{24a}$$

$$\beta_i' = \max\{\beta', \frac{\sup_{x\in\partial\mathcal{U}_{s_i}} V_2(x)}{\inf_{x\in\mathbf{R}^n\setminus\mathcal{U}_s} V_2(x)}\} \tag{24b}$$

Proof. We can derive the probability of Equation (23) following similar arguments to those in [11]. Since the deterministic prediction model of Equation (7b) is used in the stochastic Safeness Index-based LEMPC of Equation (7), it follows that there always exists a solution $u(t) = \Phi_s(\tilde{x}(t_q)) \in U$, $\forall t \in [t_q, t_{q+1})$, $q = k, \ldots, k+\tau_P-1$ that satisfies the constraints of Equation (7d–g) over the prediction horizon provided that $x(t_k), t_k \geq 0$ is inside the safe operating region $\mathcal{S}$. Therefore, this implies that the probability of recursive feasibility (i.e., Equation (23)) is equal to the probability of closed-loop process operational safety over $t \in [0, \tau_N\Delta)$, which can be obtained via the recursive application of Equation (13) with β_i and β_i' of Equation (24) and the definition of conditional probability. Additionally, it should be noted that if $x(0) \in \mathcal{S}_{2e}$, the state is not in $\partial\mathcal{U}_{s_i}$ in Equation (24). In this case, β_i' simply takes the value of β', and the probability of Equation (23) still holds since it is shown in the proof of Theorem 2 that the state either stays in $\mathcal{S}_2$ or moves into $\mathcal{S}_1$ with the probability of $1-\lambda$ (i.e., Equation (23) gives a conservative result in this case). □

Remark 6. *In Theorem 3, probabilistic process operational safety and probabilistic recursive feasibility over the operation period $t \in [0, \tau_N\Delta)$ are established for the closed-loop system of Equation (1) under the Safeness Index-based LEMPC of Equation (7). Due to the disturbance $w(t)$ with unbounded variation, the closed-loop state $x(t)$ may leave $\mathcal{S}$ at any sampling step, and thus, closed-loop process operational safety and recursive feasibility of the Safeness Index-based LEMPC of Equation (7) can only be derived in a probabilistic manner (i.e., $\forall t \in [0, \tau_N\Delta)$, these properties hold with the probability of Equation (23)). Since the existence of a feasible control action is only guaranteed in the safe operating region $\mathcal{S}$, backup safety systems should be designed to handle the process if the state exits the safe operating region. Additionally, since the probabilities of Equations (13)–(15) are less than one if $\rho_e < \rho$ and $s_e < s$, the probabilities of recursive feasibility and process operational safety for $t \in [0, \tau_N\Delta)$ decrease as the operation period $\tau_N\Delta$ becomes longer. However, it should be noted that this dependence is not unique to the MPC, but to all control designs that try to keep the process state within a specific region in state-space in the presence of stochastic disturbances with unbounded variation (i.e., the probability to keep the closed-loop state in $\mathcal{S}$ for all the remaining time of operation goes to zero at t_0 as the process operation time $\tau_N \to \infty$).*

4. Application to a Chemical Process Example

A chemical process example is used to illustrate the application of the stochastic Safeness Index-based LEMPC of Equation (7) to maintain the closed-loop state within a safe operating region in state-space in probability. Specifically, a well-mixed, non-isothermal continuous stirred tank reactor (CSTR) where an irreversible second-order exothermic reaction takes place is considered. The reaction transforms a reactant A to a product B ($A \rightarrow B$). The inlet concentration of A, the inlet temperature and the feed volumetric flow rate of the reactor are C_{A0}, T_0 and F, respectively. The CSTR is equipped with a heating jacket that supplies/removes heat at a rate Q. The CSTR dynamic model is described by the following material and energy balance equations:

$$\begin{aligned} dC_A =& \frac{F}{V_L}(C_{A0} - C_A)dt - k_0 e^{-E/RT} C_A^2 dt \\ &+ \sigma_1 (C_A - C_{As}) dw_1(t) \end{aligned} \tag{25a}$$

$$\begin{aligned} dT =& \frac{F}{V_L}(T_0 - T)dt - \frac{\Delta H k_0}{\rho_L C_p} e^{-E/RT} C_A^2 dt + \frac{Q}{\rho_L C_p V_L} dt \\ &+ \sigma_2 (T - T_s) dw_2(t) \end{aligned} \tag{25b}$$

where C_A is the concentration of reactant A in the reactor, V_L is the volume of the reacting liquid in the reactor, T is the temperature of the reactor and Q denotes the heat input rate. The concentration of reactant A in the feed is C_{A0}. The feed temperature and the volumetric flow rate are T_0 and F, respectively. The reacting liquid has a constant density of ρ_L and a heat capacity of C_p. ΔH, k_0, E and R represent the enthalpy of reaction, pre-exponential constant, activation energy and ideal gas constant, respectively. Process parameter values are given in Table 1. The disturbance terms dw_1 and dw_2 in Equation (25) are independent standard Gaussian white noise with the standard deviations $\sigma_1 = 2.5 \times 10^{-3}$ and $\sigma_2 = 0.15$, respectively. It is noted that the disturbance terms of Equation (25) vanish at the steady state.

Table 1. Parameter values of the continuous stirred tank reactor (CSTR).

$T_0 = 300$ K	$F = 5$ m^3/h
$V_L = 1$ m^3	$E = 5 \times 10^4$ kJ/kmol
$k_0 = 8.46 \times 10^6$ m^3/kmol h	$\Delta H = -1.15 \times 10^4$ kJ/kmol
$C_p = 0.231$ kJ/kg K	$R = 8.314$ kJ/kmol K
$\rho = 1000$ kg/m^3	$C_{A0_s} = 4$ kmol/m^3
$Q_s = 0.0$ kJ/h	$C_{A_s} = 1.22$ kmol/m^3
$T_s = 438$ K	

The initial steady-state of the CSTR is at $(C_{As},\ T_s) = (1.22$ kmol/m^3, 438 K), and $(C_{A0_s}\ Q_s) = (4$ kmol/m^3, 0 kJ/h). The manipulated inputs are the inlet concentration of species A and the heat input rate, which are represented by the deviation variables $u_1 = \Delta C_{A0} = C_{A0} - C_{A0_s}$ and $u_2 = \Delta Q = Q - Q_s$, respectively. The manipulated inputs are bounded as follows: $|\Delta C_{A0}| \leq 3.5$ kmol/m^3 and $|\Delta Q| \leq 5 \times 10^5$ kJ/h. Therefore, the states and the inputs of the closed-loop system are represented by $x^T = [C_A - C_{As}\ T - T_s]$ and $u^T = [\Delta C_{A0}\ \Delta Q]$, respectively.

The control objective of the stochastic Safeness Index-based LEMPC of Equation (7) is to maximize the production rate of B, while maintaining the closed-loop state trajectories in the safe operating region $\mathcal{S}$ in probability. The objective function of Equation (7a) is the production rate of B: $L_e(\tilde{x}, u) = k_0 e^{-E/RT} C_A^2$. The Lyapunov functions are designed using the standard quadratic form $V_i(x) = x^T P_i x$, $i = 1, 2$, where the positive definite matrices $P_1 = \begin{bmatrix} 1060 & 22 \\ 22 & 0.52 \end{bmatrix}$ and $P_2 = \begin{bmatrix} 1060 & 10 \\ 10 & 5 \end{bmatrix}$ are chosen to characterize

the set ϕ_d for the stochastic system of Equation (25). The nonlinear feedback controllers in [13,18] are utilized as $\Phi_n(x)$ and $\Phi_s(x)$, respectively. The level sets of the Lyapunov functions $V_1(x)$ and $V_2(x)$ are chosen as $\rho = 368$ and $s = 8100$ to create a safe operating region $\mathcal{S}$. The explicit Euler method with an integration time step of $h_c = 10^{-4}$ h is applied to numerically simulate the dynamic model of Equation (25). The nonlinear optimization problem of the stochastic Safeness Index-based LEMPC of Equation (7) is solved using the IPOPT software package [19] with the sampling period $\Delta = 10^{-2}$ h. With the fixed sampling period $\Delta = 10^{-2}$ h, $\rho = 368$ and $s = 8100$, we focus on the impact of ρ_e and s_e on probabilistic process operational safety in the following simulations.

It is first shown in Figure 4 that under the Safeness Index-based LEMPC of Equation (6) designed for the nominal system of Equation (25), the closed-loop state of the nominal system of Equation (25) stays in the safe operating region $\mathcal{S}$ within the entire operation period $t_s = 1$ h. Additionally, the Safeness Index-based LEMPC of Equation (6) is solved successfully in each iteration to obtain a feasible control action $u(t)$ that is applied in the next sampling period.

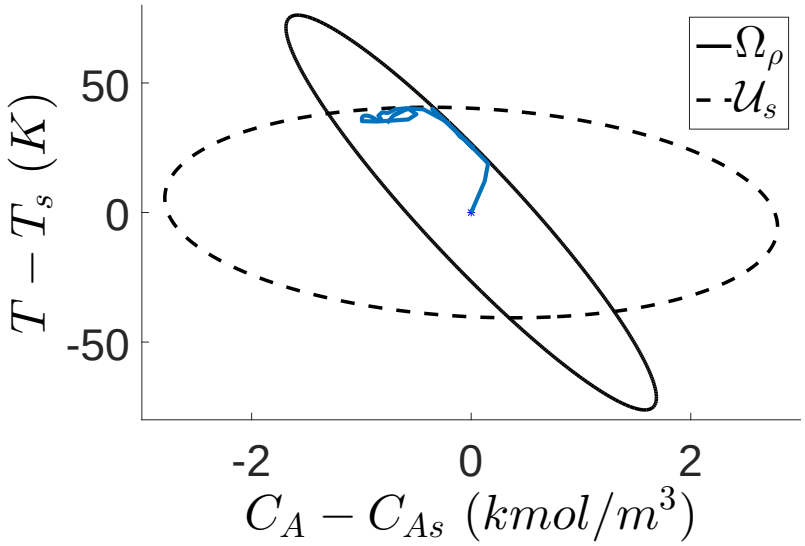

Figure 4. Closed-loop trajectory under the Safeness Index-based LEMPC of Equation (6) for the initial condition (0, 0) (in deviation variable form) with the additional material constraint: $\frac{1}{t_s}\int_0^{t_s} u_1(\tau)d\tau = 0$ kmol/m^3.

It follows that under the stochastic Safeness Index-based LEMPC of Equation (7), the state of the closed-loop system of Equation (25) stays in $\mathcal{S}$ with different probabilities for different ρ_e and s_e. To better understand the relationship between probabilistic process operational safety and the choices of ρ_e and s_e, we derived the experimental probabilities via 500 simulation runs for the same initial condition $(\Delta C_{As}, \Delta T_s) = (0$ kmol/m^3, 0 K) and different choices of ρ_e and s_e (without the material constraint applied for the nominal system). Let A_V denote the event that the closed-loop state stays in $\mathcal{S}$ over the operation period $t_s = 1$ h. The results are reported in Table 2.

Table 2. Experimental probability for different values of ρ_e and s_e.

ρ_e/ρ	s_e/s	$P(A_V)$
0.98	0.99	14.0%
0.95	0.99	63.1%
0.92	0.99	82.0%
0.92	0.97	82.8%
0.92	0.95	83.6%
0.92	0.92	85.8%

From Table 2, it is observed that with fixed s_e, $\mathbf{P}(A_V)$ becomes larger as ρ_e decreases. Likewise, with fixed ρ_e, $\mathbf{P}(A_V)$ increases as s_e decreases. It is demonstrated that a higher probability of closed-loop process operational safety of the system of Equation (25) is achieved when ρ_e and s_e are more conservative. Let $\rho_e = 320$ and $s_e = 6800$. It is obtained that the probability of the states of the closed-loop system of Equation (25) remaining in the safe operating region $\mathcal{S}$ reaches 97.4%. Additionally, the averaged total economic benefit (i.e., the time integral of the stage cost L_e over the operation period $t_s = 1$ h) is 24.3 under the Safeness Index-based LEMPC of Equation (7), which has an improvement of 81% compared to 13.4 under steady-state operation. Therefore, in this example, the closed-loop system of Equation (25) under the Safeness Index-based LEMPC achieves a relatively high probability of process safety and a satisfactory process economic performance simultaneously with $\rho_e = 320$ and $s_e = 6800$. For an actual process, additional work should likely be performed, which can use techniques like those demonstrated here, to increase the probability of the states of the closed-loop system remaining within the safe operating region to higher values considered acceptable for the process at hand given its design, hazards and the backup measures (alarms/operators, safety systems, relief systems) in place.

On the other hand, it is observed from Table 2 that decreasing ρ_e increases the probability $\mathbf{P}(A_V)$. By looking at unsafe closed-loop trajectories (i.e., trajectories that leave the safe operating region $\mathcal{S}$ under the Safeness Index-based LEMPC of Equation (7) during the operation period t_s) in 500 simulation runs (one of them is shown in Figure 5), it is observed that almost all of the unsafe trajectories leave $\mathcal{S}$ through the boundary of Ω_ρ (i.e., the right edge of Ω_ρ in Figure 5). The reason for this behavior is that the local optimum value of L_e is calculated to be at the right edge of Ω_ρ, which is shown as the yellow region in Figure 6. Therefore, under the Safeness Index-based LEMPC of Equation (7), the closed-loop trajectory is optimized to approach this high production rate region and begin circling back due to the disturbances, which leads to a higher probability of leaving the safe operating region $\mathcal{S}$ from Ω_ρ. Additionally, it is observed in Figure 6 that the production rate decreases as the safe operating region shrinks (i.e., the color becomes darker), which is consistent with the fact that smaller ρ_e and s_e lead to safer process operation, at the cost of lower economic performance.

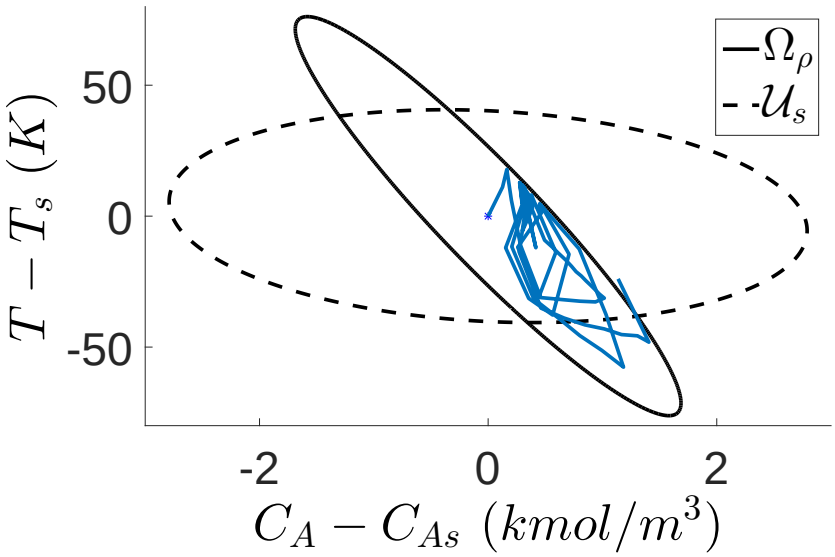

Figure 5. An example closed-loop trajectory under the Safeness Index-based LEMPC of Equation (7) for the initial condition $(0, 0)$ that leaves the safe operating region $\mathcal{S}$, in which $\rho_e = 320$ and $s_e = 6800$.

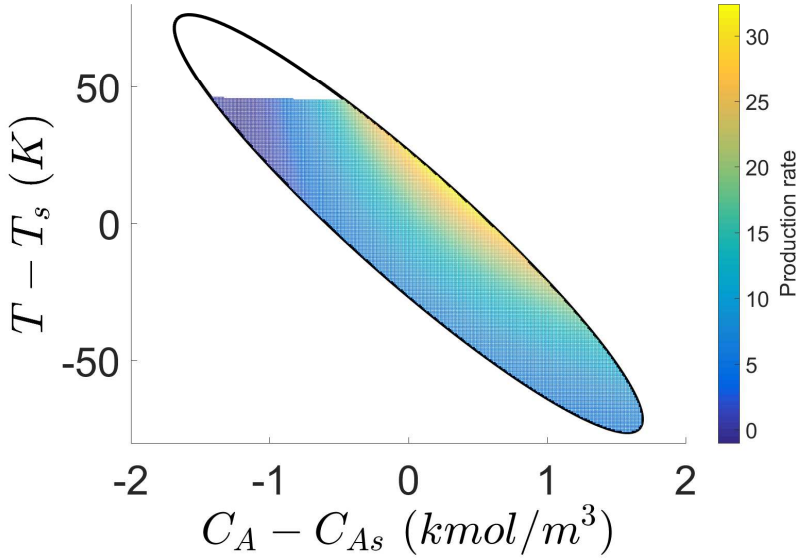

Figure 6. The production rate $L_e = k_0 e^{-E/RT} C_A^2$ within the safe operating region $\mathcal{S}$.

5. Conclusions

In this work, a Safeness Index-based LEMPC design was developed for stochastic nonlinear systems. Under the assumption of stabilizability of the origin of the stochastic nonlinear system via a stochastic Lyapunov-based control law, an economic model predictive controller was developed to account for process operational safety by utilizing Lyapunov-based constraints to maintain the closed-loop state in a safe operating region defined by a Safeness Index function. Under the stochastic Safeness Index-based LEMPC, economic optimality may be achieved with respect to the objective function and sampling period. Additionally, recursive feasibility and process operational safety of the closed-loop stochastic nonlinear system were derived in probability for a well-characterized safe operating region. A chemical reactor example was used to demonstrate the effectiveness of the proposed control method.

Author Contributions: Zhe Wu developed the main results, performed the simulation studies and prepared the initial draft of the paper. Helen Durand contributed to the theory of probabilistic process operational safety and revised this manuscript. Panagiotis D. Christofides developed the idea of Safeness Index-based LEMPC for stochastic nonlinear systems, oversaw all aspects of the research and revised this manuscript.

Acknowledgments: Financial support from the National Science Foundation and the Department of Energy is gratefully acknowledged.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Sanders, R.E. *Chemical Process Safety: Learning from Case Histories*; Butterworth-Heinemann: Oxford, UK, 2015.
2. Albalawi, F.; Durand, H.; Christofides, P.D. Process operational safety using model predictive control based on a process Safeness Index. *Comput. Chem. Eng.* **2017**, *104*, 76–88. [CrossRef]
3. Albalawi, F.; Durand, H.; Alanqar, A.; Christofides, P.D. Achieving operational process safety via model predictive control. *J. Loss Prev. Process Ind.* **2018**, *53*, 74–88. [CrossRef]
4. Heidarinejad, M.; Liu, J.; Christofides, P.D. Economic model predictive control of nonlinear process systems using Lyapunov techniques. *AIChE J.* **2012**, *58*, 855–870. [CrossRef]
5. Angeli, D.; Amrit, R.; Rawlings, J.B. On average performance and stability of economic model predictive control. *IEEE Trans. Autom. Control* **2012**, *57*, 1615–1626. [CrossRef]

6. Müller, M.A.; Angeli, D.; Allgöwer, F. Economic model predictive control with self-tuning terminal cost. *Eur. J. Control* **2013**, *19*, 408–416. [CrossRef]
7. Ellis, M.; Durand, H.; Christofides, P.D. A tutorial review of economic model predictive control methods. *J. Process Control* **2014**, *24*, 1156–1178. [CrossRef]
8. Van Hessem, D.; Bosgra, O. Stochastic closed-loop model predictive control of continuous nonlinear chemical processes. *J. Process Control* **2006**, *16*, 225–241. [CrossRef]
9. Mahmood, M.; Mhaskar, P. Lyapunov-based model predictive control of stochastic nonlinear systems. *Automatica* **2012**, *48*, 2271–2276. [CrossRef]
10. Maciejowski, J.M.; Visintini, A.L.; Lygeros, J. NMPC for complex stochastic systems using a Markov chain Monte Carlo approach. In *Assessment and Future Directions of Nonlinear Model Predictive Control*; Springer: Berlin/Heidelberg, Germany, **2007**, 269–281.
11. Wu, Z.; Zhang, J.; Zhang, Z.; Albalawi, F.; Durand, H.; Mahmood, M.; Mhaskar, P.; Christofides, P.D. Economic Model Predictive Control of Stochastic Nonlinear Systems. *AIChE J.* **2018**. [CrossRef]
12. Khasminskii, R. *Stochastic Stability of Differential Equations*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2011; Volume 66.
13. Florchinger, P. A universal formula for the stabilization of control stochastic differential equations. *Stoch. Anal. Appl.* **1993**, *11*, 155–162. [CrossRef]
14. Deng, H.; Krstic, M.; Williams, R. Stabilization of stochastic nonlinear systems driven by noise of unknown covariance. *IEEE Trans. Autom. Control* **2001**, *46*, 1237–1253. [CrossRef]
15. Wu, Z.; Albalawi, F.; Zhang, Z.; Zhang, J.; Durand, H.; Christofides, P.D. Contro Lyapunov-Barrier Function-Based Model Predictive Control of Nonlinear Systems. In Proceedings of the American Control Conference, Milwaukee, WI, USA, 27–29 June 2018; in press.
16. Ciesielski, Z.; Taylor, S.J. First passage times and sojourn times for Brownian motion in space and the exact Hausdorff measure of the sample path. *Trans. Am. Math. Soc.* **1962**, *103*, 434–450. [CrossRef]
17. Øksendal, B. Stochastic differential equations. In *Stochastic Differential Equations*; Springer: Berlin/Heidelberg, Germany, 2003; pp. 65–84.
18. Sontag, E.D. A 'universal' construction of Artstein's theorem on nonlinear stabilization. *Syst. Control Lett.* **1989**, *13*, 117–123. [CrossRef]
19. Wächter, A.; Biegler, L.T. On the implementation of an interior-point filter line-search algorithm for large-scale nonlinear programming. *Math. Progr.* **2006**, *106*, 25–57. [CrossRef]