Model-Predictive Safety Optimal Actions to Detect and Handle Process Operation Hazards

Masoud Soroush[1,*], Leila Samandari Masooleh[1], Warren D. Seider[2], Ulku Oktem[3], and Jeffrey E. Arbogast[4,5]

[1]Department of Chemical and Biological Engineering, Drexel University, Philadelphia, PA 19104, USA
[2]Department of Chemical and Biomolecular Engineering, University of Pennsylvania, Philadelphia, PA 19104-6393, USA
[3]Near-Miss Management, LLC, 1800 JFK Blvd., Suite 300, Philadelphia, PA 19103, USA
[4]American Air Liquide, Newark, DE 19702, USA
[5]Air Liquide (China) R&D Co., Ltd., Shanghai, China 201108

January 20, 2020

REVISED VERSION

Submitted for Publication in *AIChE Journal*

Keywords: Model-predictive safety, process constraints, process safety, chemical processes, receding horizon, predictive alarm

[*]Corresponding author. soroushm@drexel.edu; (215) 895-1710 (phone); (215) 895-5837 (fax)

Abstract

In 2016, we introduced the concept of model-predictive safety (MPS) [1]. MPS is a proposed innovation in functional safety systems to methodically account for process nonlinearities and variable interactions to enable predictive, prescriptive actions, while existing functional safety systems generally react when individual process variables exceed thresholds. MPS systematically utilizes a dynamic process model to detect imminent and potential future operation hazards in real time and to take optimal preventive and mitigative actions proactively. This work expands the concept of MPS and formulates two min-max optimization problems, offline solutions of which are the optimal proactive preventive and mitigating actions that MPS takes online, in response to predicted process operation hazards. A nested particle swarm optimization (PSO) algorithm is proposed to solve the min-max optimization problems. The application and performance of the min-max optimization formulations, the PSO algorithm, and MPS, applied to two chemical process examples, are shown through numerical simulations.

1 Introduction

In spite of continuous extensive efforts to improve the safety of processes, the level of human and financial losses due to incidents in the U.S. process industries is still significant (more than 50 serious accidents only over the past ten years [2]). This motivates the development of methods that predict emerging operating hazards in processes, allowing for *proactive prevention and mitigation* of the hazards [3].

Among efforts to improve process safety further, software packages have been used within the process industries [4-14] to predict frequencies and consequences of incidents based upon historical data. However, these packages are usually unable to predict the probabilities of incidents that have never happened before [4-22]. This inability points to a need for methods capable of predicting hazardous conditions in processes.

In a process, typically there are two instrumentation hardware and software systems: a control system and a safety instrumented system (SIS). A control system is used to ensure an efficient operation of the process and the production of high-quality products under normal conditions. An SIS is a functional safety system, which is used to take automatic actions (such as emergency shutdowns) needed to prevent equipment damage, environmental, and/or personnel safety consequences. An SIS is always a protection layer above the control system in a process. In addition to having the ability to override the control system (the ability to take over the actuators that the control system sends signals

to), it generally has the ability to set other process input variables. The hierarchical structure of protection layers in processes is essential, as it ensures the robustness and modularity of the process protection layers. Therefore, SISs have to meet stricter regulations and oversight (both within companies and by governments) than control systems. A conventional hierarchical process protection structure is shown in Figure S1. In such a structure, a control system and an SIS both send alarm signals to an alarm system to activate alarms to alert the process personnel to an abnormal condition. In response, the process personnel may then take corrective actions through the operator inputs (OI). In recent years, safety constraints have been included in model-predictive control (MPC) formulations to ensure MPC actions do not lead to unsafe conditions in processes that are under MPC [3, 23-26].

Dynamic first-principles process models have been used widely in design, optimization, process monitoring, model-based control, and offline safety analysis and validation of chemical and petrochemical processes. While they may not predict future process behavior *exactly*, they can be used to forecast the potential consequences of future incidents with reasonable accuracy. Such forecasts can lead to proactive actions whose consequences (outcomes) can be predicted. This combined predictive and proactive (prescriptive), real-time use of process models in process safety had not been explored until very recently [1].

Model-predictive safety (MPS)[1] represents a new paradigm in functional safety; that is, the use of model predictions to detect operation hazards before they lead to safety risks. Unlike conventional safety systems that are individually reactive to current conditions through specifically designed logic, an MPS system systematically accounts for process nonlinearities and interactions among process variables and generates predictive alarm signals alerting process personnel to imminent and potential future operation hazards. Therefore, this new paradigm in functional safety systems is analogous to the evolution in process control systems from only single-loop control (e.g., proportional-integral-derivative control) toward multivariable MPC. Figure S2 depicts a hierarchical process protection structure with an MPS system. When appropriate, the MPS system can be directly incorporated into the SIS. Herein, we expand the concepts of MPS and formulate two min-max optimization problems that are solved offline. For each process-constraint index, the formulations allow for a systematic calculation of: (a) the optimal MPS action that minimizes the highest value of the process-constraint index over a moving prediction horizon when uncertain model parameters and process variables take their nominal values, and (b) the optimal MPS action that minimizes the highest value of the process-constraint index over a moving prediction horizon when uncertain model parameters and process variables take their worst-case values. An MPS system uses the optimal MPS actions in real time to:

(i) generate the predictive definitely hazardous and potentially hazardous operation alarm signals described previously [1], and (ii) prescribe optimal proactive preventive and mitigating actions in response to the predicted process operation hazards. A particle-swarm optimization (PSO) method is proposed to solve the min-max optimization problems.

First, Section 2 briefly reviews the components of MPS [1] that are relevant to this work. Section 3 describes the two min-max optimization formulations and the PSO method. Section 4 formulates min-max problems for two chemical process examples, solves the problems using PSO, and presents the application and performance of the min-max optimization formulations as well as MPS applied to the two examples, through numerical simulations.

2 Model-Predictive Safety: Preliminaries

In this section, the concept of MPS, introduced earlier [1], is reviewed briefly and expanded. In this formulation, MPS is given the ability to set all process inputs (manipulated variables and other safety process inputs). An MPS system includes two major components: a set of process constraints and a state-estimate predictor, which is based on a process model.

2.1 Process Model

Consider a dynamic process model in the general form:

$$\frac{dx(t)}{dt} = f\big(x(t), d(t), d_m(t), p(t), u(t)\big), \qquad x(0) = x_0 \in \Omega_{x_0} \subset \mathbb{R}^{n_x}$$
$$y(t) = h\big(x(t)\big) \tag{1}$$

with the *process operation* constraints:

$$G\big(x(t), d(t), d_m(t), p(t), u(t)\big) \in \Omega_c \subset \mathbb{R}^{n_c} \tag{2}$$

where $x \in \Omega_x \subset \mathbb{R}^{n_x}$ is the vector of process state variables, $d \in \Omega_d \subset \mathbb{R}^{n_d}$ is the vector of unmeasured process input variables, $d_m \in \Omega_{d_m} \subset \mathbb{R}^{n_{d_m}}$ is the vector of measured process input variables (excluding manipulated variables and other adjustable process input variables), $p \in \Omega_p \subset \mathbb{R}^{n_p}$ is the vector process uncertain parameters, $u \in \Omega_u \subset \mathbb{R}^{n_u}$ is the vector of process input variables that MPS can set or override, and $y \in \Omega_y \subset \mathbb{R}^{n_y}$ is the vector of process output variables. The vector u includes every manipulated input (variable) that is adjusted by a control system. The sets $\Omega_x, \Omega_d, \Omega_{d_m}, \Omega_p,$ and Ω_{x_0} are closed convex sets that are hyperrectangles, each defined by the upper and lower limits of the parameters or variables that belong to the hyperrectangle. The set Ω_u consists of the corner points of a hyperrectangle. Each corner point represents an action that MPS can take. $f, h,$ and G are smooth vector functions.

The process constraints systematically include all existing process alarm thresholds of primary and secondary process variables. Also, included in this constraint formulation is the saturation of each actuator. The general constraint formulation of Eq. (2) allows for the design of MPS systems that account for process nonlinearities and interactions among process variables.

Real and hypothetical process personnel errors, process (including controller, sensor, actuator, and equipment) faults, and surrounding and feed changes can be included in the formulation through the parameters and initial conditions. For example, a parameter can be added to represent the state of health of a pump. In this case, the moving-horizon safety analyses determine whether process constraints are satisfied in the event that the pump fails. The vector of process parameters can include catalyst activity, the state of health of each process equipment item, and the process personnel inputs to the process. For each uncertain quantity, a range of possible values that each quantity can take are typically available based on historical data, operation procedures, and/or process-personnel experience.

2.2 Receding-Horizon Safety Analyses

As an MPS system generates alarm signals indicating the occurrence of present and/or future operation hazard(s), an operation hazard needs to be defined and classified in terms of its occurrence likelihood.

Definition 1: An operation hazard is said to exist when control and functional safety systems are unable to prevent the violation of a process constraint over a time horizon into the future.

Upon identification of an operation hazard, functional safety systems and/or process personnel must intervene to proactively prevent the occurrence of the hazard and mitigate its consequences.

Definition 2: The operation of a process at a time instant t is said to be *nominally* hazard-free over a time horizon of $[t, t+\tau]$, if at the time instant t there exists a feasible MPS action profile, $u(\ell|t) \in \Omega_u,\ \ell \in [t, t+\tau]$, that satisfies the following conditions:

$$G\big(\hat{x}(\ell|t), d(\ell|t), d_m(\ell|t), p(\ell|t), u(\ell|t)\big) \in \Omega_c, \quad d_m(t|t) = \tilde{d}_m(t),\ d(\ell|t) = d_n,$$
$$d_m(\ell|t) = d_{m_n},\ p(\ell|t) = p_n,\ x_0 = x_{0_n},\ \forall \ell \in [t, t+\tau] \tag{3}$$

where d_n, d_{m_n}, x_{0_n} and p_n are the nominal (typical operating) values of d, d_m, x_0 and p, respectively. Note that $\hat{x}$ represents the vector of state estimates at time ℓ given the last measurements (available at time t), and $\tilde{d}_m(t)$ denotes the vector of measurements of measurable process inputs at t [1]. A dissatisfaction of the condition of Eq. (3) indicates the existence of an operation hazard at the present time or the development of an operation hazard in the future. In other words, the conditions

allow MPS to predict the presence of *future* risks and to determine whether the functional safety system has adequate ability to maneuver away from the current and future operation hazards at the current time instant t. A dissatisfaction of the condition of Eq. (3) also indicates that no controller or functional safety system, whether traditional or model-based, can provide safe operation at a time instant in the future.

Definition 3: The operation of a process at a time instant t is said to be *absolutely* hazard-free over a time horizon of $[t, t+\tau]$, if at the time instant, t, there exists a feasible MPS action profile, $u(\ell|t) \in \Omega_u,\ \ell \in [t, t+\tau]$, that satisfies the following conditions:

$$G\big(\hat{x}(\ell|t), d(\ell|t), d_m(\ell|t), p(\ell|t), u(\ell|t)\big) \in \Omega_c,\ \ d_m(t|t) = \tilde{d}_m(t),$$
$$\forall\, d(\ell|t) \in \Omega_d, \forall d_m(\ell|t) \in \Omega_{d_m}, \forall p(\ell|t) \in \Omega_p,\ \forall x_0 \in \Omega_{x_0},\ \ \forall \ell \in [t, t+\tau] \qquad (4)$$

If the operation of a process is *absolutely* hazard-free at a time instant t, then the MPS system is able to ensure that all process constraints of Eq. (4) are satisfied over a time horizon of $[t, t+\tau]$ into the future. Note that the conditions of Eq.(4) are required to be satisfied for every $d \in \Omega_d$, every $d_m \in \Omega_{d_m}$, every $p \in \Omega_p$, and every $x_0 \in \Omega_{x_0}$. Thus, the conditions of Eq. (4) account systematically for parameter and input uncertainties.

2.3 State-Estimate Predictor

As Eqs. (3) and (4) indicate, the receding-horizon safety analyses require the present and future estimates of the process state variables. This process state estimate prediction can be achieved by simply using a process model directly (without any corrective feedback of output measurements) or by using a state estimator that takes advantage of a corrective feedback. In the former case, state estimates may not be adequately accurate to use in real-time applications. The feedback especially with integral action has several advantages such as improving the robustness of the estimates to process-model mismatch. There are several methods of state estimation. The use of an extended Luenberger observer based on an extended model (process model combined with models of every mismatch and unknown disturbance) was proposed in Ref.[1] However, the systematic design of a robust state-estimate predictor is still an open problem.

2.4 MPS Alarm Mechanisms

On the basis of the three definitions in Section 2.2, two alarm mechanisms were proposed [1]. The mechanisms at each time instant t, determine whether an MPS system is able to force the process to satisfy all conditions of Eqs. (3) and (4) over the moving time horizon $\Omega_\tau = [t, t+\tau]$. On the

dissatisfaction of a condition of Eq. (3) or (4) at a time instant t, an MPS system generates an alarm signal corresponding to the constraint:

- **Definitely Hazardous Operation** (DHO), when the operation is not *nominally* hazard-free (when a constraint of Eq. (3) is not satisfied); and
- **Potentially Hazardous Operation** (PHO), when the operation is not *absolutely* hazard-free (when a constraint of Eq. (4) is not satisfied).

The DHO alarm mechanism allows for predictively determining whether the operation is hazard-free under normal conditions (no faults or uncertainties), while the PHO alarm mechanism allows for predictively determining whether the operation is hazard-free under all real or hypothetical faults and errors accounted for in the MPS design. When the DHO alarm corresponding to a constraint is ON, the PHO alarm corresponding to the same condition is ON too. However, the converse may not be true, because a necessary condition for a DHO alarm to be OFF is that its PHO alarm counterpart be OFF.

3 Real-Time Implementation

An MPS system should determine the satisfaction of every constraint of Eqs. (3) and (4) in real time at desired time instants (to generate a DHO or PHO alarm signal whenever a constraint is not satisfied) and prescribe an optimal action when a DHO or PHO alarm signal is generated. In practice, process operation constraints of Eq. (2) can be written in the form of the inequality constraints (constraint indices):

$$\psi_i\big(\hat{x}(\ell|t), d(\ell|t), d_m(\ell|t), p(\ell|t), u(\ell|t)\big) \le 0, \quad i = 1, \cdots, n_{c,in} \tag{5}$$

where $n_{c,in}$ is the number of inequality constraints. According to Definitions 2 and 3, in real time at every desired time instant, t, an MPS system should determine whether:

(i) For every ψ_i there exists a feasible MPS action profile, $u(\ell|t) \in \Omega_u,\ \ell \in \Omega_\tau = [t, t+\tau]$, such that $\psi_i \le 0$ at every $\ell \in \Omega_\tau$ when $d_m(t|t) = \tilde{d}_m(t),\ d(\ell|t) = d_n,\ d_m(\ell|t) = d_{m_n}$, $p(\ell|t) = p_n$, and $x_0 = x_{0_n}$; and

(ii) For every ψ_i there exists a feasible MPS action profile, $u(\ell|t) \in \Omega_u,\ \ell \in [t, t+\tau]$, such that $\psi_i \le 0$ at every $\ell \in \Omega_\tau$ when $d_m(t|t) = \tilde{d}_m(t),\ \forall\, d(\ell|t) \in \Omega_d,\ \forall d_m(\ell|t) \in \Omega_{d_m}$, $\forall p(\ell|t) \in \Omega_p,$ and $\forall x_0 \in \Omega_{x_0}$.

These determinations are computationally very expensive and thus are hard to carry out in real time. This major computational difficulty is overcome using a novel approach proposed in the next section.

3.1 Combined Offline and Online Computational Approach

The main idea behind this approach is that: (i) when at a time instant t with the 'most aggressive MPS action' corresponding to ψ_i, ψ_i exceeds zero over $[t, t+\tau]$, then the DHO alarm signal corresponding to ψ_i is generated; and (ii) when at a time instant t with the 'most aggressive MPS action' and the 'worst-case values' of d, d_m, p and x_0 corresponding to ψ_i, ψ_i exceeds zero over $[t, t+\tau]$, then the PHO alarm signal corresponding to ψ_i is generated.

The corner points of the hyperrectangle Ω_u represent the actions that an MPS system can take, and the corner boundary points of Ω_{x_0}, Ω_d, Ω_{d_m}, and Ω_p that correspond to combinations of lower and upper limits of x_0, d, d_m, and p. In the case of non-complex small-scale processes, personnel knowledge of the process and/or process model predictions usually guides the identification of the combination of the lower and upper bounds for the components of x_0, d, d_m, and p that represent the 'most extreme' (worst-case) values corresponding to a constraint index. In this case, the same knowledge can be used to identify the 'most aggressive' MPS action corresponding to a constraint index. In the case of complex large-scale processes, however, these worst-case uncertainties and most aggressive MPS actions need to be calculated systematically offline using the min-max optimization problem formulations described in the next section.

3.1.1 Offline Calculations

The most aggressive (optimal) MPS action corresponding to a ψ_i is defined as the time-invariant the MPS action that minimizes the highest value of ψ_i over the moving horizon $[t, t+\tau_{s_i}]$ when $d_m(t|t) = \tilde{d}_m(t)$, $d(\ell|t) = d_n$, $d_m(\ell|t) = d_{m_n}$, $p(\ell|t) = p_n$, and $x_0 = x_{0_n}$, where $\tau_{\psi_i} = \max_j \theta_{ij}$, and θ_{ij} is the 2% settling time of ψ_i with respect to u_j. It is obtained by solving the min-max optimization problem:

$$\min_{u\in\Omega_u} \max_{t\in\Omega_{\tau_{\psi_i}}} \psi_i\big(x(t), d_n, d_{m_n}, p_n, u(t)\big) \tag{6}$$

subject to:

$$\frac{dx(t)}{dt} = f\big(x(t), d(t), d_m(t), p(t), u(t)\big), \qquad x(0) = x_0 \in \Omega_{x_0} \subset \mathbb{R}^{n_x}$$

$$y(t) = h\big(x(t)\big)$$

$$\psi_j\big(x(t), d(t), d_m(t), p(t), u(t)\big) \le 0, \quad j = 1, \cdots, n_{c,in}, \ j \neq i$$

$$\frac{du(t)}{dt} = 0$$

The infeasibility of the min-max optimization problem corresponding to a ψ_i points to the poor design of the MPS system and the need for providing the MPS system with more process input variables to set. As requested, the optimal MPS action is time-independent (is a fixed corner point of the Ω_u hyperrectangle); that is,

$$u^{*n}(t)_i = u^{*n}{}_i.$$

The most aggressive (optimal) MPS action and the worst-case values of t, x_0, d, d_m, and p corresponding to a ψ_i are, respectively, defined as the time-invariant MPS action that minimizes ψ_i, the values of t and x_0 on $\Omega_{\tau_{\psi_i}} \times \Omega_{x_0}$ that maximize ψ_i, and the time-invariant values of d, d_m, and p on $\Omega_d \times \Omega_{d_m} \times \Omega_p$ that maximize ψ_i, where $\Omega_{\tau_{\psi_i}} = [t, t + \tau_{\psi_i}]$. They are obtained by solving the following min-max optimization problem:

$$\min_{u \in \Omega_u} \quad \max_{t \in \Omega_{\tau_{\psi_i}}, d \in \Omega_d, d_m \in \Omega_{d_m}, p \in \Omega_p, x_0 \in \Omega_{x_0}} \quad \psi_i\big(x(t), d(t), d_m(t), p(t), u(t)\big) \tag{7}$$

subject to:

$$\frac{dx(t)}{dt} = f\big(x(t), d(t), d_m(t), p(t), u(t)\big), \qquad x(0) = x_0 \in \Omega_{x_0} \subset \mathbb{R}^{n_x}$$

$$y(t) = h\big(x(t)\big)$$

$$\psi_j\big(x(t), d(t), d_m(t), p(t), u(t)\big) \le 0, \quad j = 1, \cdots, n_{c,in}, \ j \ne i$$

$$\frac{d\, d(t)}{dt} = 0, \qquad \frac{d\, d_m(t)}{dt} = 0, \qquad \frac{dp(t)}{dt} = 0, \qquad \frac{du(t)}{dt} = 0$$

As requested, the optimal MPS action is time-independent (is a fixed corner point of the Ω_u hyperrectangle), and the worst-case values of $d^*(t), d_m^*(t), p^*(t)$, and x_0 are also time-independent (a fixed combination of the boundary points of the hyperrectangles); that is:

$$(d^*(t), d_m^*(t), p^*(t), x_0, u^*(t))_i = (d^*, d_m^*, p^*, x_0{}^*, u^*)_i, \qquad \forall\, t$$

3.1.2 Online Calculations

The offline calculation of the worst-case uncertainties and the most aggressive (optimal) MPS actions permits online implementation of MPS with very little computer CPU time, as the satisfaction of each process operation constraint is evaluated online only (a) one time with the nominal values of process parameters and inputs, and a corner point of Ω_u corresponding to the most aggressive action of the MPS system, for the particular process operation constraint; and (b) one time with the worst-case combination of the values that process inputs and parameters can take, and the corner point of Ω_u that corresponds to the most aggressive action of the MPS system, for the particular process operation constraint index. Thus, with the offline calculations, the implementation of an MPS system

simply requires online integration of the differential equations of a state estimator at each time instant t over a moving time horizon of $[t, t+\tau]$ at most $2n_{c,in}$ times, where τ can be much shorter than τ_{ψ_i}, $i = 1, \cdots, n_{c,in}$. Figure 1 illustrates this for one of the inequality constraints when $n_d = n_{d_m} = n_p = n_u = 2$ to determine whether an operation is *nominally* hazard-free, at a time instant t. Figure 2 illustrates the concept for one of the inequality constraints when $n_d = n_{d_m} = n_p = n_u = 2$ to determine whether an operation is *absolutely* hazard-free at a time instant t. Figure 3 depicts a block diagram that explains the implementation of an MPS system in real time. Of course, the higher is the value of τ, the more effective is MPS in preventing and mitigating accidents, but the lower is the accuracy of the alarm signals (the higher is the probability of false alarms). In contrast, MPC usually requires online integration of the same differential equations at each time instant t over a moving time horizon of $[t, t+\tau]$ significantly more than $2n_{c,in}$ times to solve an MPC optimization problem at the time instant t.

4 Numerically Solving the Min-Max Optimization Problems

A min-max optimization problem minimizes the maximum value of an objective function or a set of objective functions. Two main types of min-max optimization problems have been reported:

- Type A:

$$\min_x \max_i F_i(x),$$

subject to:

$$g(x) = 0$$
$$h(x) \leq 0$$

- Type B:

$$\min_{q \in Q} \max_{v \in V} F(q, v)$$

subject to:

$$g(q, v) = 0$$
$$h(q, v) \leq 0$$

This second type has application in decision making in the presence of uncertainty. The goal of this min-max optimization is to minimize the maximum of the objective function when optimizing variables take their worst-case combination. Min-max optimization problems of this type have been reported in many fields [27-28] for the last two decades. They are known as difficult problems to solve [29], with no general technique or algorithm to locate globally optimal solutions, especially for nonconvex problems [30]. The min-max optimization problems of MPS, Eqs. (6) and (7), are of this type in which a loss is minimized for the worst case (maximum loss) scenario.

Various approaches and methods have been proposed for solving the min-max problems, ranging from gradient-based to stochastic optimization methods. Gradient-based methods, such as successive quadratic programming (SQP), are often not suitable due to limitations, such as the unavailability of exact derivatives of objective functions and the lack of objective functions continuity [31-32].

Stochastic optimization algorithms have been found to be efficient for global optimization. They are often able to escape from local optima and show good performance uniformly across many data sets [33]. Swarm intelligence and swarm evolutionary techniques exploit social behavior and natural evolution algorithmic mechanisms, respectively. Unlike gradient-based methods, these techniques do not require objective function derivatives, and can handle discontinuous objective functions and disjoint search spaces [34]. For discrete min-max optimization problems, Herrmann[35] presented a two-space genetic algorithm (GA), and Laskari et al.[36] investigated the use of the particle-swarm optimization (PSO) method. They reported cases where SQP failed, but PSO had success rates higher than 90%. They also used a smoothing technique and found that PSO results, in many cases, were superior. Hassan et al. [37] compared the computational effectiveness and efficiency of GA and PSO using a formal hypothesis testing approach. They observed that PSO and GA were comparable in finding globally optimal solutions, but that PSO provided significantly better computational efficiencies.

Particle-swarm optimization was developed by Eberhart and Kennedy [38] inspired by the social behavior of bird flocking or fish schooling. PSO uses intuition and the social behavior of individuals to locate global optima. The particle-swarm algorithm starts with initial positioned particles, having computed objective functions, with assigned initial velocities. A particle i is defined by its position vector, z_i, and its velocity vector, v_i. In each iteration, j, the position of the particle in the next iteration, $z_i(j+1)$, is calculated according to [39]:

$$z_i(j+1) = z_i(j) + v_i(j+1) \tag{8}$$

where $z_i(j)$ is the position of the particle in the current iteration, and $v_i(j+1)$ is the velocity of the particle in the next iteration, calculated using:

$$v_i(j+1) = \omega v_i(j) + c_1 r_1(p_i(j) - x_i(j)) + c_2 r_2\big(p_g(j) - x_i(j)\big) \tag{9}$$

where $v_i(j)$ is the velocity of the particle in the current iteration; $p_i(j)$ is the best location the particle has achieved until the current iteration; $p_g(j)$ is the best location that the other particles have found until the current iteration; and c_1 and c_2 are, respectively, cognitive and social parameters, which vary

between 0 and 2. The parameters c_1 and c_2 determine the size of the step each particle takes towards its own personal best position and the overall global best position, respectively. Default values for these two parameters in PSO codes are $c_1 = c_2 = 2$. r_1 and r_2 are two random vectors whose components are assumed to be independent random variables from $U(0, 1)$. These values are different in each iteration, as they are generated randomly every time. ω is an inertia weight that maintains balance between global and local search abilities. It is usually a constant value between 0.8 and 1.2. In this work, it is set to 1.

Chen et al. [40] used the PSO method in a nested form to solve a min-max optimization problem of the second type:

$$\min_{q\in Q} \max_{v\in V} F(q, v) = \min_{q\in Q} f_{outer}(q) \tag{10}$$

where

$$f_{outer}(q) = \max_{v\in V} F(q, v) \tag{11}$$

They used two PSO algorithms, one for minimization, and the other for the maximization. For the outer minimization, particles minimize the maximum of the cost function. For each particle, the maximum is calculated using the inner PSO algorithm. As the flowchart in Figure 4 shows, calculations start with the outer function. First, the outer PSO randomly chooses n particles by assigning initial positions and velocities for every particle in the space of q. Each particle is a solution guess. Next, for each particle in the q space, the inner PSO maximizes the cost function in the domain of v. The inner function initiates iterations by assigning initial positions and velocities to every particle in the domain of v. Through a series of iterations for each outer particle, positions and velocities are updated according to Eqs. (8) and (9), and the maximization over v is performed until convergence is achieved – providing the maximum, for each outer particle, of $F(q,v)$ in Eq. (10). This procedure is repeated for every particle in the outer PSO, until the outer function converges, and the final solution of the min-max optimization is found.

5 Case Studies

The application and performance of the min-max optimization formulations as well as MPS, applied to two chemical process examples, are shown through numerical simulations in this section. One example (Process Example 1) is an isothermal continuous-stirred-tank reactor (CSTR) with series chemical reactions, and the other (Process Example 2) is a free-radical polymerization CSTR.

The resulting min-max optimization problems are solved using the nested PSO algorithm. For the first process, 100 particles and 20 max stall iterations are used, and for the second process, 200

particles and 40 max stall iterations are used. For both, default values are used for all other tuning parameters of the PSO algorithm programmed in MATLAB version R2018b. The solution of each min-max optimization problem in Process Example 1 requires just a few seconds of CPU time. For the min-max optimization problems in Process Example 2, having 17 variables, solutions were obtained using a high-performance computer cluster with Intel® Xeon® E5-2670 Sandy Bridge CPUs. The Parallel Computing Toolbox of MATLAB permitted 12 Intel CPUs to compute in parallel with a 32 GB of memory. The wall time was about 20 minutes for solving each of these min-max optimization problems.

5.1 Process Example 1: A Classical Chemical Reactor

Consider an isothermal CSTR in which the irreversible series reactions $A \rightarrow B \rightarrow C$ take place. The reactor is represented by:

$$\begin{aligned} \frac{dc_A}{dt} &= -k_1 {c_A}^2 + \left(c_{A_i} - c_A\right)F \\ \frac{dc_B}{dt} &= k_1 {c_A}^2 - k_2 c_B - c_B F \\ \frac{dc_C}{dt} &= k_2 c_B - c_C F \end{aligned} \tag{12}$$

where c_A, c_B, and c_C ($\text{kmol} \cdot \text{m}^{-3}$) are the concentrations of A, B and C in the reactor outlet stream, respectively, and F ($\text{m}^3 \cdot \text{h}^{-1}$) is the volumetric flow rate of the inlet and outlet streams. The reactor is operated at the steady state corresponding to $c_{B_{ss}} = 3\ \text{kmol} \cdot \text{m}^{-3}$ by adjusting F. The nominal values of c_{A_i}, k_1 and k_2 are $7\ \text{kmol} \cdot \text{m}^{-3}$, $6\ \text{m}^3 \cdot \text{kmol}^{-1} \cdot \text{h}^{-1}$, and $1\ \text{h}^{-1}$, respectively. Their ranges are: $5 \leq k_1 \leq 7\ \text{m}^3 \cdot \text{kmol}^{-1} \cdot \text{h}^{-1}$, $0 \leq k_2 \leq 2\ \text{h}^{-1}$, and $5 \leq c_{A_i} \leq 10\ \text{kmol} \cdot \text{m}^{-3}$. For this process, the conditions $c_B \leq 3.5\ \text{kmol} \cdot \text{m}^{-3}$ and $c_A \leq 2.0\ \text{kmol} \cdot \text{m}^{-3}$ should never be violated.

The unforced zero dynamics of the reactor are given by:

$$\begin{aligned} \frac{dc_A}{dt} &= -6{c_A}^2 + \left(c_{A_i} - c_A\right)(2{c_A}^2 - 1) \\ \frac{dc_C}{dt} &= 3 - c_C(2{c_A}^2 - 1) \end{aligned} \tag{13}$$

The eigenvalues of the Jacobian of this system are $\left[4c_{A_{ss}}\left(c_{A_i} - 3\right) - 6{c_{A_{ss}}}^2 + 1\right]$ and $[-2{c_{A_{ss}}}^2 + 1]$. At the steady state $(c_{A_{ss}}, c_{C_{ss}}, c_{A_i}) = (1, 3, 7)$, the zero dynamics are unstable, as the eigenvalues are $+11$ and -1. Consequently, c_B shows an inverse response to a step change from 1 to $2\ \text{m}^3 \cdot \text{h}^{-1}$ in F, as shown in Figure S3. When $c_{A_i} = 7\ \text{kmol} \cdot \text{m}^{-3}$, the first eigenvalue is positive for every steady state corresponding to F_{ss} ($\text{m}^3 \cdot \text{h}^{-1}$) in the range of [0, 10.45), as shown in Figure S4.

The reactor control system controls c_B by adjusting the flow rate, F, using a proportional control valve within the following range:

$$0.0 \leq F \leq F_{max} = 2.0\ \mathrm{m}^3 \cdot \mathrm{h}^{-1}$$

The control system has a simple proportional-integral (PI) controller:

$$\frac{d\omega}{dt} = -\frac{1}{\tau_I}\,\omega + \frac{1}{k_c}(F - F_{ss})$$

$$F = \mathrm{sat}\left\{F_{ss} + k_c\left(c_{B_{sp}} - c_B + \frac{1}{\tau_I}\,\omega\right)\right\}$$

where $c_{B_{sp}} = 3\ \mathrm{kmol} \cdot \mathrm{m}^{-3}$, $F_{ss} = 1\ \mathrm{m}^3 \cdot \mathrm{h}^{-1}$, $k_c = 1\ \mathrm{m}^6 \cdot \mathrm{h}^{-1} \cdot \mathrm{kmol}^{-1}$, $\tau_I = 1$ h, and

$$\mathrm{sat}\{l\} = \begin{cases} 0, & l < 0 \\ l, & 0 \leq l \leq F_{max} \\ F_{max}, & F_{max} < l \end{cases}$$

5.1.1 Model-Predictive Safety System

When one of the following constraints is violated at any moment over a receding future horizon of τ, the MPS system generates an alarm signal:

(a) Saturation alarms when:

$$F(\ell|t) \geq F_{max} = 2.0\ \mathrm{m}^3.\mathrm{h}^{-1} \tag{14}$$

$$F(\ell|t) \leq F_{min} = 0.0\ \mathrm{m}^3.\mathrm{h}^{-1} \tag{15}$$

(b) PHO and DHO alarms when:

$$\hat{c}_B(\ell|t) > 3.5\ \mathrm{kmol} \cdot \mathrm{m}^{-3} \tag{16}$$

$$\hat{c}_A(\ell|t) > 2.0\ \mathrm{kmol} \cdot \mathrm{m}^{-3} \tag{17}$$

The following constraint (alarm) indices $\psi_1, \ldots, \psi_4$ are defined:

$$\psi_1 = F(\ell|t) - 2 \tag{18}$$

$$\psi_2 = -F(\ell|t) \tag{19}$$

$$\psi_3 = \hat{c}_B(\ell|t) - 3.5 \tag{20}$$

$$\psi_4 = \hat{c}_A(\ell|t) - 2.0 \tag{21}$$

The receding prediction horizons, τ_{ψ_3}, τ_{ψ_4}, and τ are chosen to be 2.0 h, 1.0 h, and 0.2 h, respectively.

5.1.2 Min-Max Optimization

To determine whether an operation is *nominally* hazard-free, each of the constraint indices of Eqs. (20) and (21) should be checked with the nominal values of x_0, d, d_m and p, and with the most aggressive (optimal) MPS action corresponding to the condition over the receding horizon. These most aggressive MPS actions are calculated by solving the following two constrained min-max optimization problems:

$$\min_{u\in\Omega_u} \max_{t\in\Omega_{\tau_{\psi_3}}} \psi_3 = c_B(t) - 3.5 \tag{22}$$

subject to:

$$\frac{dc_A(t)}{dt} = -k_1 c_A(t)^2 + \left(c_{A_i}(t) - c_A(t)\right)F(t)$$
$$\frac{dc_B(t)}{dt} = k_1 c_A(t)^2 - k_2 c_B(t) - c_B(t)F(t)$$
$$\frac{dc_C(t)}{dt} = k_2 c_B(t) - c_C(t)F(t)$$

$$\psi_1 = F(t) - 2 \le 0$$
$$\psi_2 = -F(t) \le 0$$
$$\psi_4 = c_A(t) - 2.0 \le 0$$

and

$$\min_{u\in\Omega_u} \max_{t\in\Omega_{\tau_{\psi_4}}} \psi_4 = c_A(t) - 2.0 \tag{23}$$

subject to:

$$\frac{dc_A(t)}{dt} = -k_1 c_A(t)^2 + \left(c_{A_i}(t) - c_A(t)\right)F(t)$$
$$\frac{dc_B(t)}{dt} = k_1 c_A(t)^2 - k_2 c_B(t) - c_B(t)F(t)$$
$$\frac{dc_C(t)}{dt} = k_2 c_B(t) - c_C(t)F(t)$$

$$\psi_1 = F(t) - 2 \le 0$$
$$\psi_2 = -F(t) \le 0$$
$$\psi_3 = c_B(t) - 3.5 \le 0$$

where $u = F,\ \Omega_u = [0,\ 2],\ \ \Omega_{\tau_{\psi_3}} = [0,\ 2.0]$, and $\Omega_{\tau_{\psi_4}} = [0,\ 1.0]$.

By applying the nested PSO algorithm, these two optimization problems were solved. When k_1, k_2 and C_{Ai} take their nominal values, in both cases the algorithm found that the optimal MPS action corresponds to an inlet flow rate, *F*, of zero: $F^{*n} = 0$. The MPS system applied these to the reactor model; the simulation results shown in Figure S5 confirm that the nested PSO algorithm indeed solved the two min-max optimization problems; in both cases $F^{*n} = 0$ minimizes both constraint indices.

To determine whether an operation is *absolutely* hazard-free, the MPS system should check each of the constraint indices of Eqs. (20) ad (21) with the corresponding worst-case values of $d,\ d_m$,

p and x_0 and the optimal MPS actions. The worst-case combinations and their corresponding optimal MPS actions were calculated by solving the following two min-max optimization problems:

$$\min_{u\in\Omega_u} \max_{t\in\Omega_{\tau_{\psi_3}},d\in\Omega_d,p\in\Omega_p,x_0\in\Omega_{x_0}} \psi_3 = c_B(t) - 3.5 \tag{24}$$

subject to:

$$\frac{dc_A(t)}{dt} = -k_1 c_A(t)^2 + \left(c_{A_i}(t) - c_A(t)\right)F(t)$$
$$\frac{dc_B(t)}{dt} = k_1 c_A(t)^2 - k_2 c_B(t) - c_B(t)F(t)$$
$$\frac{dc_C(t)}{dt} = k_2 c_B(t) - c_C(t)F(t)$$

$$\psi_1 = F(t) - 2 \le 0$$
$$\psi_2 = -F(t) \le 0$$
$$\psi_4 = c_A(t) - 2.0 \le 0$$

and

$$\min_{u\in\Omega_u} \max_{t\in\Omega_{\tau_{\psi_4}},d\in\Omega_d,p\in\Omega_p,x_0\in\Omega_{x_0}} \psi_4 = c_A(t) - 2.0 \tag{25}$$

subject to:

$$\frac{dc_A(t)}{dt} = -k_1 c_A(t)^2 + \left(c_{A_i}(t) - c_A(t)\right)F(t)$$
$$\frac{dc_B(t)}{dt} = k_1 c_A(t)^2 - k_2 c_B(t) - c_B(t)F(t)$$
$$\frac{dc_C(t)}{dt} = k_2 c_B(t) - c_C(t)F(t)$$

$$\psi_1 = F(t) - 2 \le 0$$
$$\psi_2 = -F(t) \le 0$$
$$\psi_3 = c_B(t) - 3.5 \le 0$$

where $d = c_{A_i},\ \Omega_d = [5,\ 10],\ p = [k_1 \quad k_2]^T$, and $\Omega_p = [5,\ 7] \times [0,\ 2]$.

The nested PSO algorithm found that:

- In the case of the constraint index of Eq.(20), the worst combination of uncertainties is $c_{A_i} = 10,\ k_1 = 7,$ and $k_2 = 0$, and the optimal MPS action is $F = 0$.
- In the case of the constraint index of Eq.(21), the worst combination of uncertainties is $c_{A_i} = 10,\ k_1 = 5,$ and $k_2 =$ any value in [0, 2] and the optimal MPS action is $F = 0$.

The simulation results shown in Figure S6 again confirm that the nested PSO algorithm solved the two min-max optimization problems; in both cases $F^* = 0$ minimizes both constraint indices.

5.1.3 State Estimate Predictor

The MPS system uses the following state estimator to predict the future values of the state variables online[1] when the manipulated variable takes the optimal MPS value corresponding to each constraint index:

$$\frac{d\hat{c}_A(\ell|t)}{dt} = -k_1\hat{c}_A(\ell|t)^2 + \left(c_{A_i}(\ell|t) - \hat{c}_A(\ell|t)\right)F(\ell|t) + L_1\left(c_B(t|t) - \hat{c}_B(t|t)\right) + \hat{\xi}_{x_1}(\ell|t)$$

$$\frac{d\hat{c}_B(\ell|t)}{dt} = k_1\hat{c}_A(\ell|t)^2 - k_2\hat{c}_B(\ell|t) - \hat{c}_B(\ell|t)F(\ell|t) + L_2(c_B(t|t) - \hat{c}_B(t|t))$$

$$\frac{d\hat{c}_C(\ell|t)}{dt} = k_2\hat{c}_B(\ell|t) - \hat{c}_C(\ell|t)F(\ell|t) + L_3\left(c_B(t|t) - \hat{c}_B(t|t)\right)$$

$$\frac{d\hat{\xi}_{x_1}(\ell|t)}{dt} = L_4\left(c_B(t|t) - \hat{c}_B(t|t)\right)$$

5.1.4 Application of MPS

To test the MPS system, the process is assumed to undergo an unmeasured disturbance in the form of a step change in c_{A_i} from 7 to 9 $\text{kmol} \cdot \text{m}^{-3}$ at time $t = 2$ h. An SIS activates an alarm when ψ_3 exceeds zero in real time. However, MPS sets the feed flow rate to zero when the predicted future value of ψ_3 exceeds zero; that is, it sets the feed flow rate to zero before the SIS sets the current value of ψ_3 to zero. Figure 5 depicts C_A and C_B in the absence of the disturbance. The MPS system activates an DHO alarm when the constraint of Eq. (20) or (21) is violated with the optimal MPS action and the nominal values of the parameters and unmeasured disturbance, over the receding horizon of $[t, t+\tau]$. The thick blue lines in Figure 6 represent variations of the two constraint indices of the actual process under the PI controller. Figure 6 also shows the future values of the two constraint indices predicted at time instants 2.0, 2.1, 2.2, 2.3, 2.4 and 2.5 h using the state estimate predictor in Section 5.1.3, the nominal values of the uncertain quantities, and the optimal MPS action corresponding to each constraint index. It shows that none of the constraints are violated, indicating that the operation is nominally hazard free.

The MPS system activates a PHO alarm when the constraint of Eq. (20) or (21) is violated with its corresponding optimal MPS action and the worst combination of uncertainties. The thick blue lines in Figure 7 represent variations of the two constraint indices of the actual process under the PI controller. Figure 7 also shows the future values of the two constraint indices predicted at time instants 2.0, 2.1, 2.2, 2.3, 2.4 and 2.5 h using the state estimate predictor in Section 5.1.3, and the worst-case values of the uncertain quantities and the optimal MPS action corresponding to each constraint index.

It shows that the constraint index ψ_3 exceeds zero at $t = 2.09$, leading to the activation of the PHO alarm corresponding to the constraint index ψ_3 and setting the inlet stream flow rate to zero. In this case study, the uncertainties in the state estimator initial conditions were not considered. Such uncertainties can be easily handled by considering the most extreme combination of the parameter values and state-estimator initial conditions.

Figure S7 depicts the concentrations of A and B in the presence of a disturbance in the reactor. As Figure S7 shows, at $t = 2.5$ hr, the predicted concentration of B exceeds 3.5 $\text{kmol} \cdot \text{m}^{-3}$, resulting in the MPS system activating an alarm and setting the inlet flow rate to zero. With the action taken by the MPS system the constraint index ψ_3 is violated at $t = 2.09$ hr (Figure 7), leading to the activation of the PHO alarm corresponding to constraint ψ_3 by the MPS system. This case clearly demonstrates the ability of MPS in predicting the occurrence of operation hazards before the hazards really happen.

5.2 Process Example 2: A Continuous Stirred-Tank Polymerization Reactor

Consider a continuous stirred-tank jacketed polymerization reactor in which free-radical solution polymerization of methyl methacrylate (MMA) initiated by azo-bis-isobutyronitrile in toluene takes place [41]. The polymerization reactions are listed in Table S1. Under assumptions such as: (i) no gel or glass effect, (ii) the quasi-steady-state-approximation, (iii) constant density and heat capacity of the reacting mixture, (iv) a well-insulated reactor, and (v) perfect mixing, the dynamics of the continuous-stirred-tank reactor are described by:

$$
\begin{aligned}
V\frac{dc_M}{dt} &= -(k_P + k_{f_m})c_M RV + F_{M_i}c_{M_i} - Fc_M, && c_M(0) = 0 \\
V\frac{dc_I}{dt} &= -k_I c_I V + F_{I_i}c_{I_i} - Fc_I, && c_I(0) = 0 \\
V\frac{dc_i}{dt} &= -k_i c_i RV + F_{M_i}c_{i_i} - Fc_i && c_i(0) = 0 \\
C\rho V\frac{dT}{dt} &= k_P c_M RV\Delta H + FC\rho(T_i - T) + US(T_j - T), && T(0) = T_{sp} \\
\frac{dT_j}{dt} &= \frac{US(T - T_j) + Q}{c_j m_j}, && T_j(0) = T_{j,0}
\end{aligned}
\tag{26}
$$

where

$$F = F_{M_i} + F_{I_i},$$

$$k_j = z_j \exp\left(\frac{-E_j}{R_C T}\right), \quad j = I, P, t, i, f_m$$

$$Q = \Delta H_s \dot{m}_s + F_{cw}\rho_{cw}c_{cw}(T_{cw} - T_j)$$

Applying the quasi-steady-state assumption to the rate of change of the molar concentration of the free radicals leads to:

$$R = \frac{-k_i c_i + \sqrt{(k_i c_i)^2 + 8 f k_t k_I c_I}}{2k_t}$$

The variables are defined in the Nomenclature. Online measurements of $T_j, T,\ T_i, F_{M_i}\ F_{I_i},\ F_{cw}$, and $\dot{m}_S$ are assumed to be available. The reactor control system adjusts the cooling water flow rate, F_{cw}, and the steam mass flow rate, $\dot{m}_s$, using proportional valves within the following ranges:

$$0 \le F_{cw} \le F_{cw_{max}} = 2.22 \times 10^{-4}\ \mathrm{m^3 \cdot s^{-1}}$$

$$0 \le \dot{m}_s \le \dot{m}_{s\ max} = 0.15\ \mathrm{kg \cdot s^{-1}}$$

In addition to overriding these two manipulated variables, the MPS system can set the inlet monomer and initiator flow rates, F_{M_i} and F_{I_i} using ON-OFF valves within the following ranges:

$$0 \le F_{M_i} \le F_{M_i\ max} = 8.3 \times 10^{-4}\ \mathrm{m^3 \cdot s^{-1}}$$

$$0 \le\ F_{I_i} \le F_{I_{i\ max}} =\ 1.6 \times 10^{-5}\ \mathrm{m^3 \cdot s^{-1}}$$

The remaining nominal values of the reactor model parameters are given in Tables 1a and 1b.

5.2.1 Model-Predictive Safety System

For this process, the constraint indices are:

$$\psi_1 = F_{cw}(\ell|t) - F_{cw_{max}} \quad (27)$$

$$\psi_2 = -\ F_{cw}(\ell|t) \quad (28)$$

$$\psi_3 = \dot{m}_s(\ell|t) - \dot{m}_{s\ max} \quad (29)$$

$$\psi_4 =\ -\dot{m}_s(\ell|t) \quad (30)$$

$$\psi_5 = F_{M_i}(\ell|t) - F_{M_i\ max} \quad (31)$$

$$\psi_6 = -F_{M_i}(\ell|t) \quad (32)$$

$$\psi_7 =\ F_{I_i}(\ell|t) - F_{I_{i_{max}}} \quad (33)$$

$$\psi_8 =\ -\ F_{I_i}(\ell|t) \quad (34)$$

$$\psi_9 = \hat{c}_m(\ell|t) - 0.6 \quad (35)$$

$$\psi_{10} = \hat{c}_I(\ell|t) - 0.02 \quad (36)$$

$$\psi_{11} =\ \hat{c}_i(\ell|t) - 3 \times 10^{-4} \quad (37)$$

$$\psi_{12} = \hat{T}(\ell|t) - 373.2 \quad (38)$$

$$\psi_{13} = \hat{T}_j(\ell|t) - 393.2 \tag{39}$$

When at a time instant t the projected value of a constraint index over the receding prediction horizon $[t, t+\tau]$ exceeds zero, the MPS system activates the corresponding alarm.

The reactor temperature is controlled using a cascade control system consisting of two PI controllers:

$$\frac{d\omega_1}{dt} = -\frac{1}{\tau_{I_1}}\,\omega_1 + \frac{1}{k_{c_1}}\left(T_{j_{sp}} - T_{j_{ss}}\right)$$

$$\frac{d\omega_2}{dt} = -\frac{1}{\tau_{I_2}}\,\omega_2 + \frac{1}{k_{c_2}}(Q - Q_{ss})$$

$$T_{j_{sp}} = \mathrm{sat}_{T_{j_{sp}}}\left\{T_{j_{ss}} + k_{c_1}\left(T_{sp} - T + \frac{1}{\tau_{I_1}}\,\omega_1\right)\right\}$$

$$Q = \mathrm{sat}_{Q}\left\{Q_{ss} + k_{c_2}\left(T_{j_{sp}} - T_j + \frac{1}{\tau_{I_2}}\,\omega_2\right)\right\}$$

where $T_{sp} = 363.2$ K, $Q_{ss} = -50.16$ kJ $\cdot$ s^{-1}, $k_{c_1} = 1$, $\tau_{I_1} = 5 \times 10^3$ s, $k_{c_2} = 200$ kJ $\cdot$ s^{-1} $\cdot$ K^{-1}, $\tau_{I_2} = 1 \times 10^5$ s, and

$$\mathrm{sat}_Q\{l\} = \begin{cases} Q_{min}, & l < Q_{min} \\ l, & Q_{min} \le l \le Q_{max} \\ Q_{max}, & Q_{max} < l \end{cases}$$

$$\mathrm{sat}_{T_{j_{sp}}}\{l\} = \begin{cases} 0, & l < 0 \\ l, & 0 \le l \le T_{j_{max}} \\ T_{j_{max}}, & T_{j_{max}} < l \end{cases}$$

where $Q_{max} = \Delta H_s \dot{m}_{s_{max}}$ and $Q_{min} = F_{cw_{max}} \rho_{cw} c_{cw} (T_{cw} - T_j)$. The primary and secondary controllers control the reactor and jacket temperatures, respectively. Their manipulated variables are the jacket temperature setpoint, $T_{j_{sp}}$, and the rate of energy supplied to/removed from the reactor jacket, Q.

5.2.2 Min-Max Optimization

To determine whether an operation is *nominally* hazard-free, the MPS system should check each condition of Eqs. (27) – (39) with the nominal values of x_0, d, d_m and p, and with the most aggressive (optimal) MPS action corresponding to that condition. The optimal MPS actions are calculated by solving the optimization problems:

$$\min_{u \in \Omega_u} \max_{t \in \Omega_{\tau_i}} \psi_i\big(x(t), d_n, d_{m_n}, p_n, u(t)\big), \qquad i = 1, \cdots, 13 \tag{40}$$

subject to the process dynamics and the remaining constraints. To solve this set of optimization problems, we applied the nested PSO algorithm. The results indicate when the initial conditions, frequency factors, and activation energies take their nominal values, the optimal MPS action corresponding to this condition is: the maximum coolant flow rate, and the minimum steam, monomer flow rates, and initiator solution.

To determine whether an operation is *absolutely* hazard-free, the MPS system should check each condition of Eqs. (27) – (39) with the corresponding worst-case values of $d,\ d_m,\ p$ and x_0 and with the corresponding optimal MPS action. Each of the worst-case combinations and its corresponding optimal MPS action are calculated using:

$$\min_{u\in\Omega_u} \max_{t\in\Omega_{\tau_i}, d\in\Omega_d, d_m\in\Omega_{d_m}, p\in\Omega_p, x_0\in\Omega_{x_0}} \psi_i\big(x(t), d(t), d_m(t), p(t), u(t)\big), \quad i = 1,\cdots,13 \qquad (41)$$

subject to the process dynamics and the remaining constraints. For each of these constraint indices, the min-max optimization is solved by applying the nested PSO algorithm. To solve these min-max problems, all of the uncertain parameters, in a lumped vector, are adjusted to maximize the inner function and calculate the most aggressive action that the manipulated variables can take. The min-max optimization results are given in Tables 2–5. A summary of the results is as follows.

- Reactor temperature upper-limit constraint index: The worst-case scenario occurs when the inlet monomer and initiator concentrations take their maximum values, and the inhibitor inlet concentration takes its minimum value. Worst-case values of the initial conditions are listed in Table 3. The optimal MPS action is the maximum cooling water flow rate, and the minimum steam, initiator solution, and monomer flow rates.
- Monomer concentration upper-limit constraint index: The worst-case scenario occurs when the inlet monomer and inhibitor concentrations take their maximum values, and the inlet initiator takes any value within $[0\ \ 10]$. Worst-case values of the initial conditions are listed in Table 4. The optimal MPS action is the maximum cooling water and initiator solution flow rates and the minimum monomer and steam flow rates.
- Initiator concentration upper-limit constraint index: The worst-case scenario happens when the inhibitor inlet concentration takes its maximum value, the initiation reaction frequency factor takes its minimum value, and the initiation reaction activation energy takes its maximum value. It is entirely independent of all other parameters. The optimal MPS action corresponding to this worst combination is the minimum initiator solution and steam flow rates and the maximum monomer and cooling water flow rates.

- Inhibitor concentration upper-limit constraint index: The worst-case scenario occurs when the inhibitor inlet concentration is at its maximum. The other worse-case values are given in Table 5. For this case, the optimal MPS action is the minimum monomer and steam flow rates and the maximum initiator solution and cooling water flow rates.

5.2.3 State Estimate Predictor

The following state estimator is used to calculate future estimates of the state variables when the MPS outputs take their optimal values corresponding to each constraint index:

$$\begin{aligned}
\frac{d\hat{c}_M(\ell|t)}{d\ell} &= -[\hat{k}_P(\ell|t)+\hat{k}_{f_m}(\ell|t)]\hat{c}_M(\ell|t)\hat{R}(\ell|t)+\frac{F_{M_i}(\ell|t)c_{M_i}(\ell|t)-F(\ell|t)\hat{c}_M(\ell|t)}{V} \\
&\quad +\eta_1, && \hat{c}_M(0|0)=\hat{c}_{M,0} \\
\frac{d\hat{c}_I(\ell|t)}{d\ell} &= -\hat{k}_I(\ell|t)\hat{c}_I(\ell|t)+\frac{\left(F_{I_i}(\ell|t)c_{I_i}(\ell|t)-F(\ell|t)\hat{c}_I(\ell|t)\right)}{V}+\eta_2, && \hat{c}_I(0|0)=\hat{c}_{I,0} \\
\frac{d\hat{c}_i(\ell|t)}{d\ell} &= -\hat{k}_i(\ell|t)\hat{c}_i(\ell|t)\hat{R}(\ell|t)+\frac{\left(F_{M_i}(\ell|t)c_{i_i}(\ell|t)-F(\ell|t)\hat{c}_i(\ell|t)\right)}{V}+\hat{\xi}_{x_1}(\ell|t)+\eta_3, && \hat{c}_i(0|0)=\hat{c}_{i,0} \\
\frac{d\hat{T}(\ell|t)}{d\ell} &= \hat{k}_P(\ell|t)\hat{c}_M(\ell|t)\hat{R}(\ell|t)\frac{\Delta H}{C\rho}+F(\ell|t)\frac{\left(T_i(\ell|t)-\hat{T}(\ell|t)\right)}{V}+\frac{US\left(\hat{T}_j(\ell|t)-\hat{T}(\ell|t)\right)}{C\rho V} \\
&\quad +\eta_4, && \hat{T}(0|0)=\hat{T}_0 \\
\frac{d\hat{T}_j(\ell|t)}{d\ell} &= \frac{US\left(\hat{T}(\ell|t)-\hat{T}_j(\ell|t)\right)+\Delta H_s\dot{m}_s(\ell|t)+F_{cw}(\ell|t)\rho_{cw}c_{cw}\left(T_{cw}-\hat{T}_j(\ell|t)\right)}{c_j m_j}+\eta_5, && \hat{T}_j(0|0)=\hat{T}_{j,0} \\
\frac{d\hat{\xi}_{x_1}(\ell|t)}{d\ell} &= \eta_6, && \hat{\xi}_{x_1}(0|0)=0
\end{aligned} \tag{42}$$

where

$$\eta_i = L_{i1}\left(T(t|t)-\hat{T}(t|t)\right)+L_{i2}\left(T_j(t|t)-\hat{T}_j(t|t)\right), \quad i=1,\cdots,6$$

$$\hat{k}_j(\ell|t)=z_j\exp\left(\frac{-E_j}{R\hat{T}(\ell|t)}\right), \quad j=I,P,t,i,f_m$$

$$\hat{R}(\ell|t)=\frac{-\hat{k}_i(\ell|t)\hat{c}_i(\ell|t)+\sqrt{\left(\hat{k}_i(\ell|t)\hat{c}_i(\ell|t)\right)^2+8f\hat{k}_t(\ell|t)\hat{k}_I(\ell|t)\hat{c}_I(\ell|t)}}{2\hat{k}_t(\ell|t)}$$

The estimator gain matrix elements are selected such that all eigenvalues of the Jacobian matrix of the estimator error dynamics have negative real parts and have the same order of magnitude. The values of the gain matrix elements are given in Table 6.

5.2.4 Application of MPS

To test the MPS system, two (normal and abnormal) operations are simulated. In the normal operation, the reactor undergoes startup in the absence of any inhibitors in the monomer or initiator solution inlet stream. The thick blue lines in Figure 8 represent variations of the five constraint indices of the actual process under the control system. Figure 8 also shows the future values of the five constraint indices predicted at the five time instants using the state estimate predictor in Section 5.2.3, and the optimal MPS action corresponding to each constraint index. The receding prediction horizon, τ, was chosen to be 0.2 h. It shows that during the normal operation (in the absence of the inhibitor), none of constraints of Eqs. (27)-(39) are violated; that is, the operation is nominally hazard free.

The thick blue lines in Figure 9 represent variations of the five constraint indices of the actual process under the control system. Figure 9 also shows the future values of the five constraint indices predicted at five time instants using the state estimate predictor in Section 5.2.3, and the worst-case values of the uncertain quantities and the optimal MPS action corresponding to each constraint index. As can be seen during normal operation, no alarms are activated as none of constraints of Eqs. (27)-(39) are violated. It indicates that the operation is absolutely hazard free.

In the abnormal operation, when the reactor is at steady state the concentration of the inhibitor in the monomer feed stream increases from 0 to 0.03 $\mathrm{kmol \cdot m^{-3}}$ (disturbance). In this case, as shown in Figure 10, the operation is nominally hazard free, because none of the constraint index predictions take a value of zero or higher. Figure 11 shows the projections of several constraint indices with the optimal MPS action corresponding to the constraint index and the worst-case values of the uncertain quantities. It depicts the constraint index ψ_9 exceeds zero at $t = 0.76$ h. Upon this violation, MPS generates the PHO alarm signal corresponding to the constraint index ψ_9 and sets the monomer inlet flow rate to zero and the initiator solution flow rate to its maximum as long as the constraint index ψ_{10} does not exceed zero, as calculated in the min-max optimization section. Even with this action taken by the MPS system, the violation of the upper bound on the monomer concentration cannot be prevented. In this case study, uncertainties in the state-estimator initial conditions were not considered. Such uncertainties can be easily handled by considering the most extreme combination of the parameter values and state-estimator initial conditions.

Figures S8 shows the concentrations of the unreacted monomer, initiator, and inhibitor in the reactor, and the reactor and jacket temperatures during the first two hours of operation after the reactor reaches steady-state conditions in the presence of the disturbance. As Figure S8 shows, at $t = 1.5$ h the monomer upper bound (0.6 $\mathrm{kmol \cdot m^{-3}}$) is violated, resulting in the MPS system generating an monomer concentration alarm signal. As Figure 11 shows, the future value of the constraint index ψ_9

first exceeds zero at $t = 0.76$ hr, leading to the MPS system activating the PHO alarm corresponding to the constraint index ψ_9. As can be seen, the MPS system predicts the future violation of the upper bound on the monomer concentration long before the concentration actually exceeds its limit in real time.

6 Conclusion

MPS can play a critical role in the petroleum, chemical and petrochemical industries. It *can be adapted easily to other industries such as the food, nuclear, aircraft, and petroleum industries,* to identify imminent and potential future operation hazards. It is a new paradigm in functional safety; that is, the design and use of predictive and proactive (prescriptive) functional safety systems that account for process nonlinearities and interactions among process variables. Existing functional safety systems typically do not account for these process characteristics and are not predictive. We envision that an MPS system will sit above a conventional functional safety system much like MPC that sits above a conventional control system.

The concept of MPS was expanded and min-max optimization problems were formulated herein. The problems are solved offline to calculate systematically (a) the optimal MPS action that minimizes each process-constraint index when uncertain model parameters take their nominal values, and (b) the optimal MPS action that minimizes each process-constraint index when uncertain model parameters take their worst-case values. To solve min-max optimization problems, a nested PSO algorithm was implemented. The min-max formulations were applied to two process examples, a classical chemical reactor with series reactions and a free-radical polymerization reactor, and the resulting min-max problems were solved using the nested PSO algorithm. Simulation results showed that the algorithm solves the min-max optimization problems reliably.

Acknowledgement

This material is based upon work supported by the U.S. National Science Foundation under Grant Nos. CBET–1704915 and CBET–1704833. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation. The authors would like to thank Ahmad A. Shamsabadi and Hossein Riazi for their help with the process simulations conducted in this work.

Nomenclature

c Heat capacity of reacting mixture, $\mathrm{kJ \cdot kg^{-1} \cdot K^{-1}}$

c_{cw} Heat capacity of cooling water, $\mathrm{kJ \cdot kg^{-1} \cdot K^{-1}}$

c_j Heat capacity of the reactor jacket, $\mathrm{kJ \cdot kg^{-1} \cdot K^{-1}}$

c_{M_i} Molar concentration of monomer in the monomer feed stream, $k\mathrm{mol \cdot m^{-3}}$

c_{I_i} Molar concentration of initiator in the initiator feed stream, $\mathrm{kmol \cdot m^{-3}}$

c_{i_i} Molar concentration of inhibitor in the monomer feed stream, $\mathrm{kmol \cdot m^{-3}}$

D_n Dead polymer chain with n monomer units

E_{f_m} Chain-transfer-to-monomer reaction activation energy, $\mathrm{kJ \cdot kmol^{-1}}$

E_I Initiation reaction activation energy, $\mathrm{kJ \cdot kmol^{-1}}$

E_i Inhibition reaction activation energy, $\mathrm{kJ \cdot kmol^{-1}}$

E_P Propagation reaction activation energy, $\mathrm{kJ \cdot kmol^{-1}}$

E_t Termination reaction activation energy, $k\mathrm{J \cdot kmol^{-1}}$

F_{cw} Cooling water volumetric flow rate, $\mathrm{m^3.s^{-1}}$

F_{I_i} Volumetric flow rate of initiator-solution feed stream, $\mathrm{m^3.s^{-1}}$

F_{M_i} Volumetric flow rate of monomer feed stream, $\mathrm{m^3.s^{-1}}$

f Initiator efficiency

I_2 Initiator

i Inhibitor

L_{ij} Observer gain matrix entries

k_{f_m} Chain-transfer-to-monomer reaction rate constant, $\mathrm{m^3 \cdot kmol^{-1} \cdot s^{-1}}$

k_I Initiation reaction rate constant, $\mathrm{s^{-1}}$

k_i Inhibition reaction rate constant, $\mathrm{m^3 \cdot kmol^{-1} \cdot s^{-1}}$

k_P Propagation reaction rate constant, $\mathrm{m^3 \cdot kmol^{-1} \cdot s^{-1}}$

k_t Termination reaction rate constant, $\mathrm{m^3 \cdot kmol^{-1} \cdot s^{-1}}$

m_j Mass of the reactor jacket, kg

$\dot{m}_s$ Mass flow rate of steam, $\mathrm{kg \cdot s^{-1}}$

R Molar concentration of free radicals, $\mathrm{kmol \cdot m^{-3}}$

R_c Gas constant, $\mathrm{J \cdot mol^{-1}K^{-1}}$

S Reactor-jacket heat-transfer surface area, $\mathrm{m^2}$

T Reactor temperature, K

T_i Temperature of the inlet stream, K

T_j Jacket temperature, K

T_{cw} Cooling water temperature, K

T_{sp} Reactor temperature set point, K

U Reactor-jacket overall heat-transfer coefficient, $\mathrm{kJ.K^{-1}.s^{-1}.m^{-2}}$

V Volume of reacting mixture, $\mathrm{m^3}$

z_{f_m} Chain-transfer-to-monomer reaction frequency factor, $\mathrm{m^3 \cdot kmol^{-1} \cdot s^{-1}}$

z_I Initiation reaction frequency factor, $\mathrm{s^{-1}}$

z_i Inhibition reaction frequency factor, $\mathrm{m^3 \cdot kmol^{-1} \cdot s^{-1}}$

z_P Propagation reaction frequency factor, $\mathrm{m^3 \cdot kmol^{-1} \cdot s^{-1}}$

z_t Termination reaction frequency factor, $\mathrm{m^3 \cdot kmol^{-1} \cdot s^{-1}}$

Greek

ΔH Heat of propagation reactions, $\mathrm{kJ \cdot kmol^{-1}}$

ΔH_s Steam latent heat, $\mathrm{kJ \cdot kg^{-1}}$

ρ Density of the reacting mixture, $\mathrm{kg \cdot m^{-3}}$

ρ_{cw} Density of cooling water, $\mathrm{kg \cdot m^{-3}}$

τ Online prediction horizon, s

τ_{ψ_i} Offline prediction horizon for the inequality constraint index ψ_i

References

1. Ahooyi, T. M.; Soroush, M.; Arbogast, J. E.; Seider, W. D.; Oktem, U. G., Model-Predictive Safety System for Proactive Detection of Operation Hazards. *AIChE Journal* **2016**, *62*, 2024-2042.
2. Zadeh, L.; Whalen, B., On Optimal Control and Linear Programming. *IRE Transactions on Automatic Control* **1962**, *7*, 45-46.
3. Leveson, N. G.; Stephanopoulos, G., A System-Theoretic, Control-Inspired View and Approach to Process Safety. *AIChE Journal* **2014**, *60*, 2-14.
4. Garcia, C. E.; Morari, M., Internal Model Control. A Unifying Review and Some New Results. *Industrial & Engineering Chemistry Process Design and Development* **1982**, *21*, 308-323.
5. Bequette, B. W., Non-Linear Model Predictive Control: A Personal Retrospective. *The canadian journal of chemical engineering* **2007**, *85*, 408-415.
6. Allgöwer, F.; Zheng, A., *Nonlinear Model Predictive Control*; Birkhäuser, 2012; Vol. 26.
7. Findeisen, R.; Allgöwer, F.; Biegler, L. T., *Assessment and Future Directions of Nonlinear Model Predictive Control*; Springer, 2007; Vol. 358.
8. Kouvaritakis, B.; Cannon, M., *Non-Linear Predictive Control: Theory and Practice*; Iet, 2001.
9. Garcia, C. E.; Prett, D. M.; Morari, M., Model Predictive Control: Theory and Practice—a Survey. *Automatica* **1989**, *25*, 335-348.

10. Ferramosca, A.; Rawlings, J. B.; Limón, D.; Camacho, E. F. In *Economic Mpc for a Changing Economic Criterion*, Decision and Control (CDC), 2010 49th IEEE Conference on, IEEE: 2010; pp 6131-6136.
11. Touretzky, C. R.; Baldea, M., Integrating Scheduling and Control for Economic Mpc of Buildings with Energy Storage. *Journal of Process Control* **2014**, *24*, 1292-1300.
12. Heidarinejad, M.; Liu, J.; Christofides, P. D., State-Estimation-Based Economic Model Predictive Control of Nonlinear Systems. *Systems & Control Letters* **2012**, *61*, 926-935.
13. Mesbah, A., Stochastic Model Predictive Control: An Overview and Perspectives for Future Research. *IEEE Control Systems* **2016**, *36*, 30-44.
14. Mesbah, A.; Streif, S.; Findeisen, R.; Braatz, R. D. In *Stochastic Nonlinear Model Predictive Control with Probabilistic Constraints*, American Control Conference (ACC), 2014, IEEE: 2014; pp 2413-2419.
15. Qin, S. J.; Badgwell, T. A., A Survey of Industrial Model Predictive Control Technology. *Control engineering practice* **2003**, *11*, 733-764.
16. Garriga, J. L.; Soroush, M., Model Predictive Control Tuning Methods: A Review. *Industrial & Engineering Chemistry Research* **2010**, *49*, 3505-3515.
17. Cutler, C. R., and B. L. Ramaker In *Dynamic Matrix Control - a Computer Control Algorithm*, Proceedings of the Joint Automatic Control Conference, San Francisco, CA, AIChE: San Francisco, CA, 1980.
18. Morrison, L. M., Best Practices in Incident Investigation in the Chemical Process Industries with Examples from the Industry Sector and Specifically from Nova Chemicals. *Journal of hazardous Materials* **2004**, *111*, 161-166.
19. Pariyani, A.; Seider, W. D.; Oktem, U. G.; Soroush, M., Incidents Investigation and Dynamic Analysis of Large Alarm Databases in Chemical Plants: A Fluidized-Catalytic-Cracking Unit Case Study. *Industrial & Engineering Chemistry Research* **2010**, *49*, 8062-8079.
20. Pariyani, A.; Seider, W. D.; Oktem, U. G.; Soroush, M., Dynamic Risk Analysis Using Alarm Databases to Improve Process Safety and Product Quality: Part I—Data Compaction. *AIChE Journal* **2012**, *58*, 812-825.
21. Steinbach, J., *Safety Assessment for Chemical Processes*; John Wiley & Sons, 2008.
22. Ramiro, J. S.; Aísa, P. B., *Risk Analysis and Reduction in the Chemical Process Industry*; Springer Science & Business Media, 2012.
23. Albalawi, F.; Durand, H.; Christofides, P. D., Process Operational Safety Using Model Predictive Control Based on a Process Safeness Index. *Computers & Chemical Engineering* **2017**, *104*, 76-88.
24. Allen, J. T.; El-Farra, N. H., A Model-Based Framework for Fault Estimation and Accommodation Applied to Distributed Energy Resources. *Renewable energy* **2017**, *100*, 35-43.
25. Albalawi, F.; Alanqar, A.; Durand, H.; Christofides, P. D., A Feedback Control Framework for Safe and Economically-Optimal Operation of Nonlinear Processes. *AIChE Journal* **2016**, *62*, 2391-2409.
26. Zhang, Z.; Wu, Z.; Durand, H.; Albalawi, F.; Christofides, P. D., On Integration of Feedback Control and Safety Systems: Analyzing Two Chemical Process Applications. *Chemical Engineering Research and Design* **2018**, *132*, 616-626.
27. Rapoport, E. Y., Minimax Optimization of Stationary States in Systems with Distributed Parameters. *Journal of Computer and Systems Sciences International* **2013**, *52*, 165-179.
28. Baums, A., Minimax Method in Optimizing Energy Consumption in Real-Time Embedded Systems. *Automatic Control and Computer Sciences* **2009**, *43*, 57-62.

29. El Ghaoui, L.; Lebret, H., Robust Solutions to Least-Squares Problems with Uncertain Data. *SIAM Journal on matrix analysis and applications* **1997**, *18*, 1035-1064.
30. Rodriguez, M.; Jones, B.; Borror, C. M.; Montgomery, D. C., Generating and Assessing Exact G-Optimal Designs. *Journal of quality technology* **2010**, *42*, 3-20.
31. Bertsekas, D., Approximation Procedures Based on the Method of Multipliers. *Journal of Optimization Theory and Applications* **1977**, *23*, 487-510.
32. Bertsekas, D., A New Algorithm for Solution of Resistive Networks Involving Diodes. *IEEE Transactions on Circuits and Systems* **1976**, *23*, 599-608.
33. Hoos, H. H.; Stützle, T., *Stochastic Local Search: Foundations and Applications*; Elsevier, 2004.
34. Eberhart, R. C.; Shi, Y.; Kennedy, J., *Swarm Intelligence*; Elsevier, 2001.
35. Herrmann, J. W. In *A Genetic Algorithm for Minimax Optimization Problems*, Proceedings of the 1999 Congress on Evolutionary Computation-CEC99 (Cat. No. 99TH8406), IEEE: 1999; pp 1099-1103.
36. Laskari, E.; Parsopoulos, K.; Vrahatis, M. In *Particle Swarm Optimization for Minimax Problems*, Proceedings of the 2002 Congress on Evolutionary Computation. CEC'02 (Cat. No. 02TH8600), IEEE: 2002; pp 1576-1581.
37. Hassan, R.; Cohanim, B.; De Weck, O.; Venter, G. In *A Comparison of Particle Swarm Optimization and the Genetic Algorithm*, 46th AIAA/ASME/ASCE/AHS/ASC structures, structural dynamics and materials conference, 2005; p 1897.
38. Eberhart, R.; Kennedy, J. In *Particle Swarm Optimization*, Proceedings of the IEEE international conference on neural networks, Citeseer: 1995; pp 1942-1948.
39. Kennedy, J. In *The Behavior of Particles*, International Conference on Evolutionary Programming, Springer: 1998; pp 579-589.
40. Chen, R.-B.; Chang, S.-P.; Wang, W.; Tung, H.-C.; Wong, W. K., Minimax Optimal Designs Via Particle Swarm Optimization Methods. *Statistics and Computing* **2015**, *25*, 975-988.
41. Soroush, M.; Kravaris, C., Nonlinear Control of a Batch Polymerization Reactor: An Experimental Study. *AIChE Journal* **1992**, *38*, 1429-1448.
42. Cutié, S. S.; Henton, D. E.; Powell, C.; Reim, R. E.; Smith, P. B.; Staples, T. L., The Effects of Mehq on the Polymerization of Acrylic Acid in the Preparation of Superabsorbent Gels. *Journal of applied polymer science* **1997**, *64*, 577-589.
43. Ototake, N.; Lueno, F.; Terada, H.; Uraguchi, Y., Rate of Termination in Bulk Polymerization of Mma Initiated by Aibn and Bpo. *Journal of Chemical Engineering of Japan* **1968**, *1*, 67-72.
44. Beuermann, S.; Buback, M., Rate Coefficients of Free-Radical Polymerization Deduced from Pulsed Laser Experiments. *Progress in Polymer Science* **2002**, *27*, 191-254.
45. Piton, M. C.; Winnik, M. A.; Davis, T. P.; O'driscoll, K. F., Copolymerization Kinetics of 4-Methoxystyrene with Methyl Methacrylate and 4-Methoxystyrene with Styrene: A Test of the Penultimate Model. *Journal of Polymer Science Part A: Polymer Chemistry* **1990**, *28*, 2097-2106.
46. Li, R.; Schork, F. J., Modeling of the Inhibition Mechanism of Acrylic Acid Polymerization. *Industrial & engineering chemistry research* **2006**, *45*, 3001-3008.
47. Dubikhin, V.; Knerel'man, E.; Nazina, L.; Prokudin, V.; Shastin, A.; Shunina, I.; Nazin, G., Thermal Decomposition of Solid Azobisisobutyronitrile. *Kinetics and Catalysis* **2013**, *54*, 18-21.
48. Levy, L. B., Inhibition of Acrylic Acid Polymerization by Phenothiazine and P-Methoxyphenol. Ii. Catalytic Inhibition by Phenothiazine. *Journal of Polymer Science Part A: Polymer Chemistry* **1992**, *30*, 569-576.

49. Victoria-Valenzuela, D.; Herrera-Ordonez, J.; Luna-Barcenas, G.; Verros, G. D.; Achilias, D. S., Bulk Free Radical Polymerization of Methyl Methacrylate and Vinyl Acetate: A Comparative Study. *Macromolecular Reaction Engineering* **2016**, *10*, 577-587.
50. Sangster, D. F.; Feldthusen, J.; Strauch, J.; Fellows, C. M., Measurement of Transfer Coefficients to Monomer for N-Butyl Methacrylate by Molecular Weight Distributions from Emulsion Polymerization. *Macromolecular Chemistry and Physics* **2008**, *209*, 1612-1627.

Table 1a: Nominal Values of the Polymerization Reactor Model Parameters.

Parameter	Value	Unit	Ref.
z_t	9.800×10^7	$\mathrm{m^3 \cdot kmol^{-1} \cdot s^{-1}}$	41
z_P	4.917×10^5	$\mathrm{m^3 \cdot kmol^{-1} \cdot s^{-1}}$	41
z_I	1.053×10^{15}	$\mathrm{s^{-1}}$	41
z_i	7.623×10^9	$\mathrm{m^3 \cdot kmol^{-1} \cdot s^{-1}}$	42
z_{f_m}	4.660×10^9	$\mathrm{m^3 \cdot kmol^{-1} \cdot s^{-1}}$	41
E_t	2.944×10^3	$\mathrm{kJ \cdot kmol^{-1}}$	41
E_P	1.828×10^4	$\mathrm{kJ \cdot kmol^{-1}}$	41
E_I	1.288×10^5	$\mathrm{kJ \cdot kmol^{-1}}$	41
E_i	2.390×10^4	$\mathrm{kJ \cdot kmol^{-1}}$	42
E_{f_m}	7.440×10^4	$\mathrm{kJ \cdot kmol^{-1}}$	41
c	2.200×10^0	$\mathrm{kJ \cdot kg^{-1} \cdot K^{-1}}$	41
ΔH	5.780×10^4	$\mathrm{kJ \cdot kmol^{-1}}$	41
f	5.800×10^{-1}		41
ρ	9.300×10^2	$\mathrm{kg \cdot m^{-3}}$	41
M_M	1.001×10^2	$\mathrm{kg \cdot kmol^{-1}}$	41
M_I	1.642×10^2	$\mathrm{kg \cdot kmol^{-1}}$	41
c_{I_i}	5.000×10^0	$\mathrm{kmol \cdot m^{-3}}$	
c_{i_i}	0.000×10^0	$\mathrm{kmol \cdot m^{-3}}$	
c_{M_i}	5.000×10^0	$\mathrm{kmol \cdot m^{-3}}$	
c_{I_0}	5.000×10^{-2}	$\mathrm{kmol \cdot m^{-3}}$	
c_{i_0}	0.000×10^0	$\mathrm{kmol \cdot m^{-3}}$	
c_{M_0}	0.000×10^0	$\mathrm{kmol \cdot m^{-3}}$	
T_0	3.430×10^2	K	

Table 1b: Nominal Values of the Other Polymerization Reactor Model Parameters.

Parameter	Value	Unit
T_i	2.932×10^2	K
U	3.000×10^{-1}	$\mathrm{kJ.K^{-1}.s^{-1}.m^{-2}}$
$T_{j,0}$	3.630×10^2	K
T_{sp}	3.632×10^2	K
ΔH_s	2.257×10^3	$\mathrm{kJ \cdot kg^{-1}}$
T_{cw}	2.882×10^2	K
ρ_{cw}	9.980×10^2	$\mathrm{kg \cdot m^{-3}}$
c_{cw}	4.180×10^0	$\mathrm{kJ \cdot kg^{-1} \cdot K^{-1}}$
c_j	2.200×10^0	$\mathrm{kJ \cdot kg^{-1} \cdot K^{-1}}$
S	1.000×10^1	$\mathrm{m^2}$

V	1.000×10^{1}	m^3
m_j	1.114×10^{4}	kg

Table 2: Ranges for the Polymerization Reactor Parameters.

Parameter	Lower value	Upper value	Unit	Ref.
z_t	3.500×10^{6}	4.900×10^{9}	$\mathrm{m}^3 \cdot \mathrm{kmol}^{-1} \cdot \mathrm{s}^{-1}$	42-44
z_P	4.917×10^{5}	6.600×10^{5}	$\mathrm{m}^3 \cdot \mathrm{kmol}^{-1} \cdot \mathrm{s}^{-1}$	42-45
z_I	4.160×10^{12}	1.000×10^{16}	s^{-1}	41, 46-47
z_i	4.800×10^{8}	7.600×10^{9}	$\mathrm{m}^3 \cdot \mathrm{kmol}^{-1} \cdot \mathrm{s}^{-1}$	42-48
z_{f_m}	2.000×10^{5}	4.660×10^{9}	$\mathrm{m}^3 \cdot \mathrm{kmol}^{-1} \cdot \mathrm{s}^{-1}$	41, 49-50
E_t	4.000×10^{2}	1.190×10^{4}	$\mathrm{kJ} \cdot \mathrm{kmol}^{-1}$	42-44
E_P	1.800×10^{4}	2.236×10^{4}	$\mathrm{kJ} \cdot \mathrm{kmol}^{-1}$	42-45
E_I	1.200×10^{5}	1.300×10^{5}	$\mathrm{kJ} \cdot \mathrm{kmol}^{-1}$	41, 46-47
E_i	2.300×10^{4}	2.500×10^{4}	$\mathrm{kJ} \cdot \mathrm{kmol}^{-1}$	42-48
E_{f_m}	2.030×10^{4}	7.440×10^{4}	$\mathrm{kJ} \cdot \mathrm{kmol}^{-1}$	41, 49-50
c_{I_i}	0.000×10^{0}	1.000×10^{1}	$\mathrm{kmol} \cdot \mathrm{m}^{-3}$	
c_{i_i}	0.000×10^{0}	1.860×10^{-2}	$\mathrm{kmol} \cdot \mathrm{m}^{-3}$	
c_{M_i}	0.000×10^{0}	9.300×10^{0}	$\mathrm{kmol} \cdot \mathrm{m}^{-3}$	

Table 3: Worst-Case Parameter Values Corresponding to the Polymerization Reactor Temperature Constraint Index.

Parameter	Value	Unit
z_t	3.500×10^{6}	$\mathrm{m}^3 \cdot \mathrm{kmol}^{-1} \cdot \mathrm{s}^{-1}$
z_P	6.600×10^{5}	$\mathrm{m}^3 \cdot \mathrm{kmol}^{-1} \cdot \mathrm{s}^{-1}$
z_I	4.160×10^{12}	s^{-1}
z_i	$4.800 \times 10^{8} - 7.600 \times 10^{9}$	$\mathrm{m}^3 \cdot \mathrm{kmol}^{-1} \cdot \mathrm{s}^{-1}$
z_{f_m}	$2.000 \times 10^{5} - 4.660 \times 10^{9}$	$\mathrm{m}^3 \cdot \mathrm{kmol}^{-1} \cdot \mathrm{s}^{-1}$
E_t	1.190×10^{4}	$\mathrm{kJ} \cdot \mathrm{kmol}^{-1}$
E_P	1.800×10^{4}	$\mathrm{kJ} \cdot \mathrm{kmol}^{-1}$
E_I	1.300×10^{5}	$\mathrm{kJ} \cdot \mathrm{kmol}^{-1}$
E_i	$2.300 \times 10^{4} - 2.500 \times 10^{4}$	$\mathrm{kJ} \cdot \mathrm{kmol}^{-1}$
E_{f_m}	7.440×10^{4}	$\mathrm{kJ} \cdot \mathrm{kmol}^{-1}$

Table 4: Worst-Case Parameter Values Corresponding to the Monomer Concentration Constraint Index.

Parameter	Value	Unit
z_t	4.900×10^{9}	$\mathrm{m}^3 \cdot \mathrm{kmol}^{-1} \cdot \mathrm{s}^{-1}$
z_P	4.917×10^{5}	$\mathrm{m}^3 \cdot \mathrm{kmol}^{-1} \cdot \mathrm{s}^{-1}$
z_I	4.160×10^{12}	s^{-1}
z_i	7.600×10^{9}	$\mathrm{m}^3 \cdot \mathrm{kmol}^{-1} \cdot \mathrm{s}^{-1}$
z_{f_m}	2.000×10^{5}	$\mathrm{m}^3 \cdot \mathrm{kmol}^{-1} \cdot \mathrm{s}^{-1}$
E_t	4.000×10^{2}	$\mathrm{kJ} \cdot \mathrm{kmol}^{-1}$
E_P	2.236×10^{4}	$\mathrm{kJ} \cdot \mathrm{kmol}^{-1}$
E_I	1.300×10^{5}	$\mathrm{kJ} \cdot \mathrm{kmol}^{-1}$
E_i	2.300×10^{4}	$\mathrm{kJ} \cdot \mathrm{kmol}^{-1}$
E_{f_m}	7.440×10^{4}	$\mathrm{kJ} \cdot \mathrm{kmol}^{-1}$

Table 5: Worst-Case Parameter Values Corresponding to the Inhibitor Concentration Constraint Index.

Parameter	Value	Unit
z_t	4.900×10^9	$\mathrm{m^3 \cdot kmol^{-1} \cdot s^{-1}}$
z_P	$4.917 \times 10^5 - 6.600 \times 10^5$	$\mathrm{m^3 \cdot kmol^{-1} \cdot s^{-1}}$
z_I	4.160×10^{12}	$\mathrm{s^{-1}}$
z_i	4.800×10^8	$\mathrm{m^3 \cdot kmol^{-1} \cdot s^{-1}}$
z_{f_m}	$2.000 \times 10^5 - 4.660 \times 10^9$	$\mathrm{m^3 \cdot kmol^{-1} \cdot s^{-1}}$
E_t	4.000×10^2	$\mathrm{kJ \cdot kmol^{-1}}$
E_P	$1.828 \times 10^4 - 2.236 \times 10^4$	$\mathrm{kJ \cdot kmol^{-1}}$
E_I	1.300×10^5	$\mathrm{kJ \cdot kmol^{-1}}$
E_i	2.500×10^4	$\mathrm{kJ \cdot kmol^{-1}}$
E_{f_m}	$2.030 \times 10^4 - 7.440 \times 10^4$	$\mathrm{kJ \cdot kmol^{-1}}$

Table 6: State-estimator Gain.

i	1	2	3	4	5	6
L_{i1}	0.88	7.46	0.00	8.88	0.79	0.01
L_{i2}	1.45	2.31	0.34	3.48	1.41	6.23

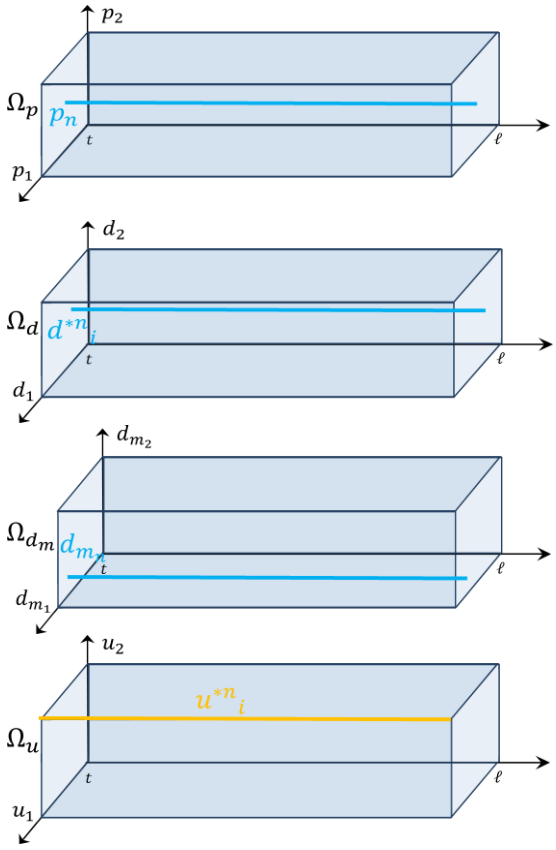

Figure 1: The optimal MPS action corresponding to a constraint index when $n_d = n_{d_m} = n_p = n_u = 2$; the u profile is calculated offline and is used online to determine whether MPS should generate a DHO signal.

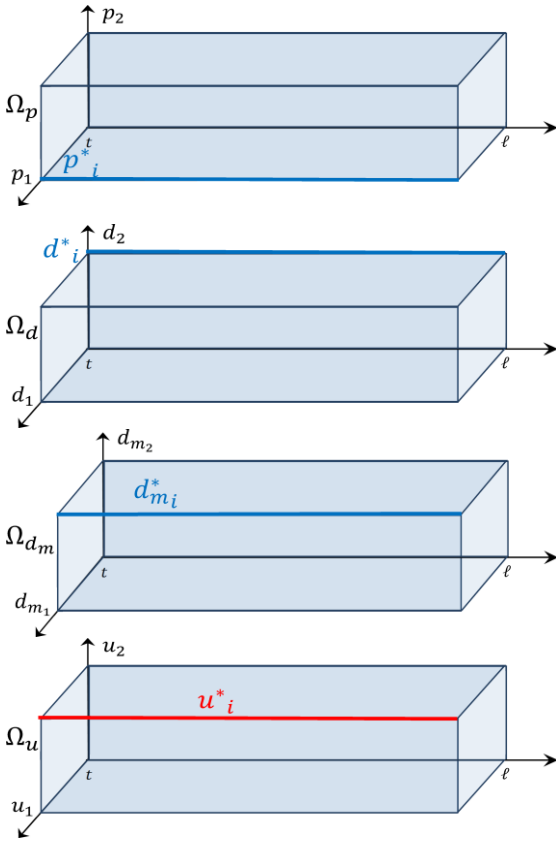

Figure 2: The worst-case values of $p, d,$ and $d_m,$ and the optimal MPS control action corresponding to a constraint index when $n_p = n_d = n_{d_m} = n_u = 2$; the d, p, d_m and u profiles are calculated offline and are used online to determine whether MPS should generate a PHO signal.

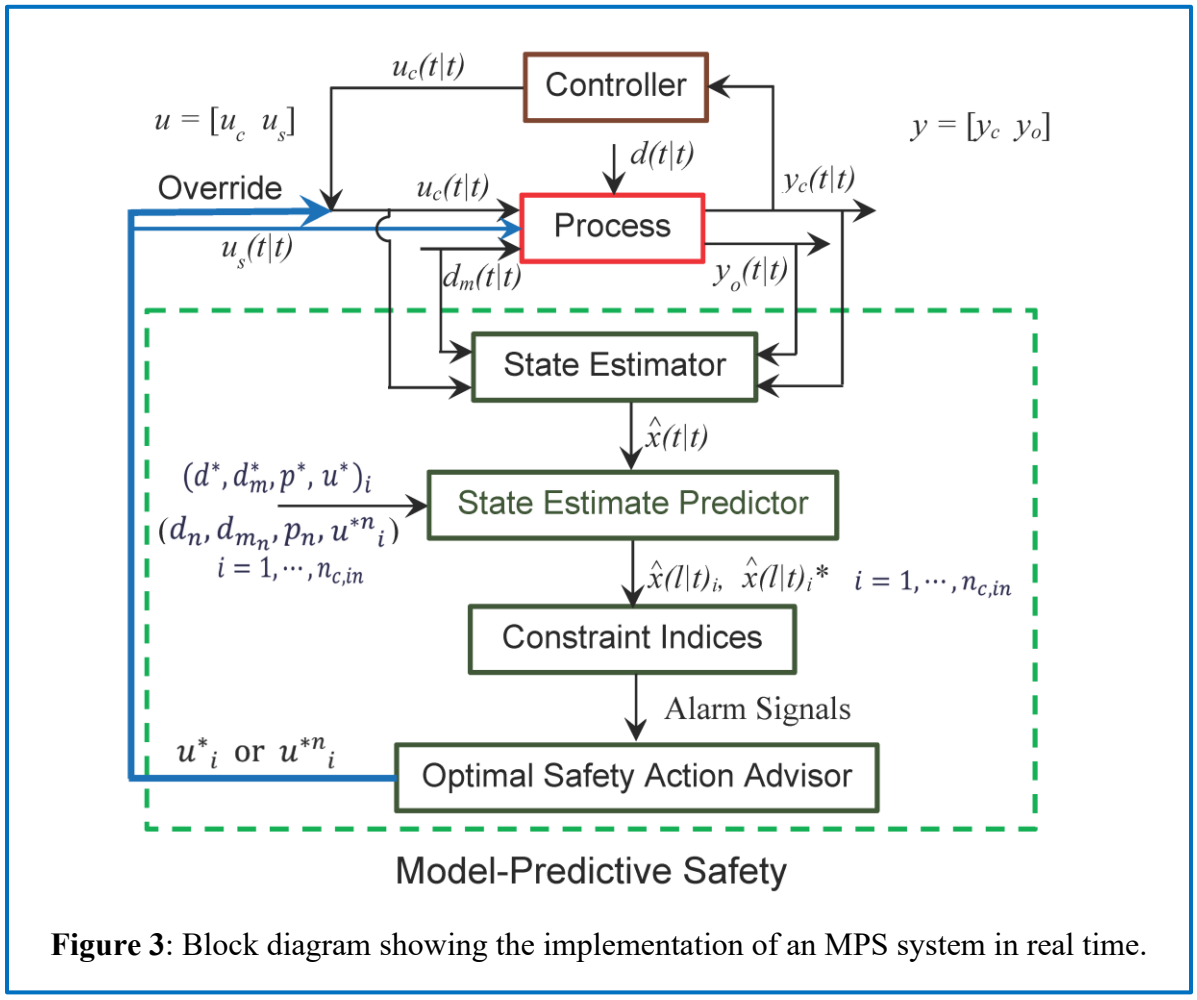

Figure 3: Block diagram showing the implementation of an MPS system in real time.

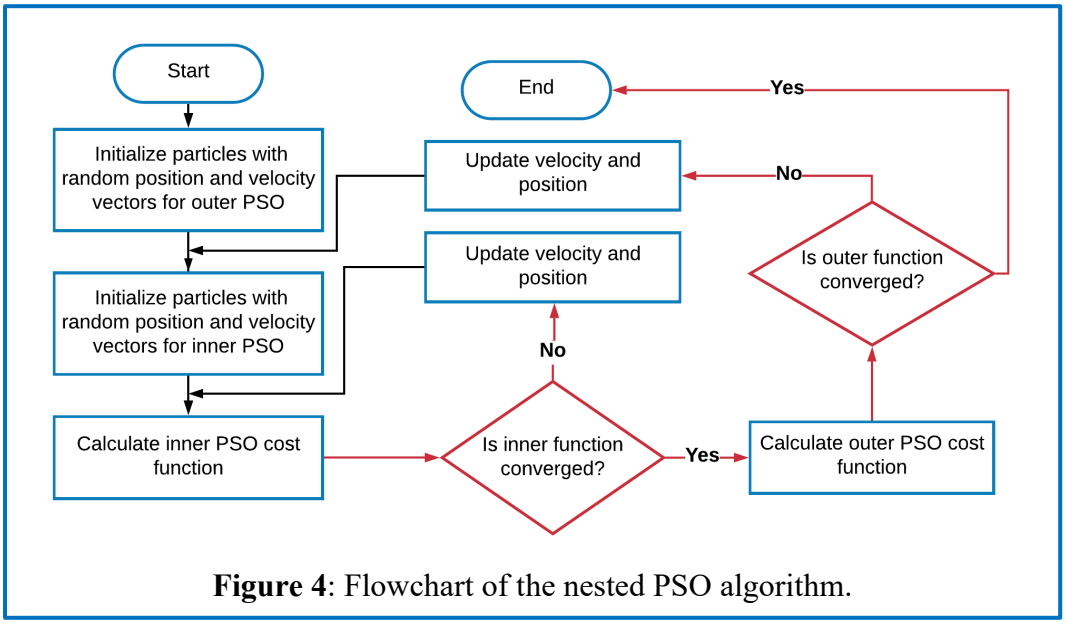

Figure 4: Flowchart of the nested PSO algorithm.

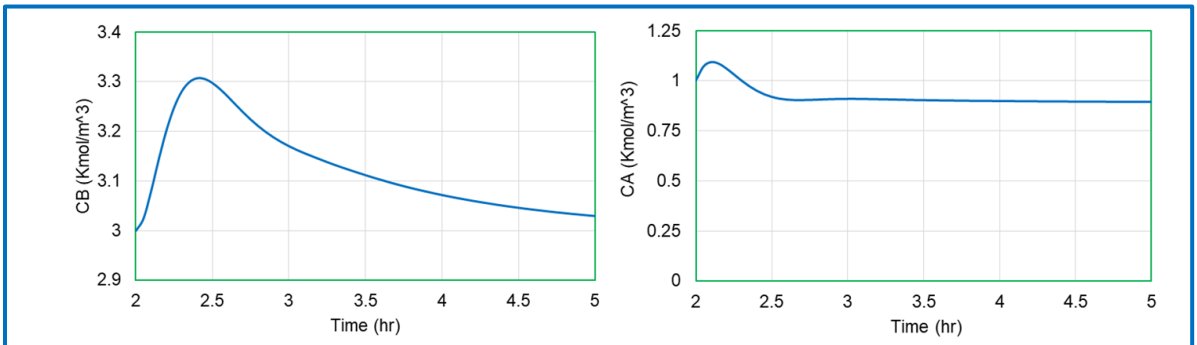

Figure 5: The reactor state in the absence of the disturbance (under hazard-free operation conditions).

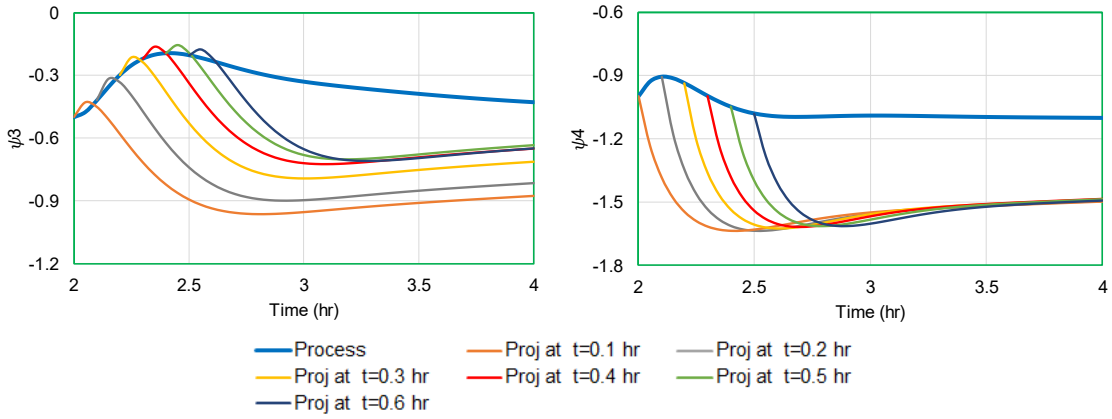

Figure 6: Real-time and projected values of the two constraint indices indicating the operation is nominally hazard free.

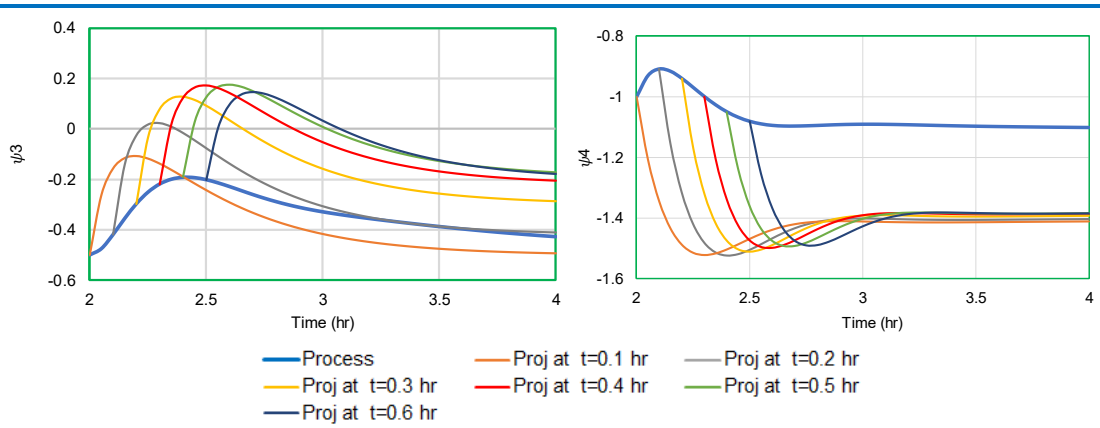

Figure 7: Real time and projected values of the constraint indices when applying the PHO alarm mechanism.

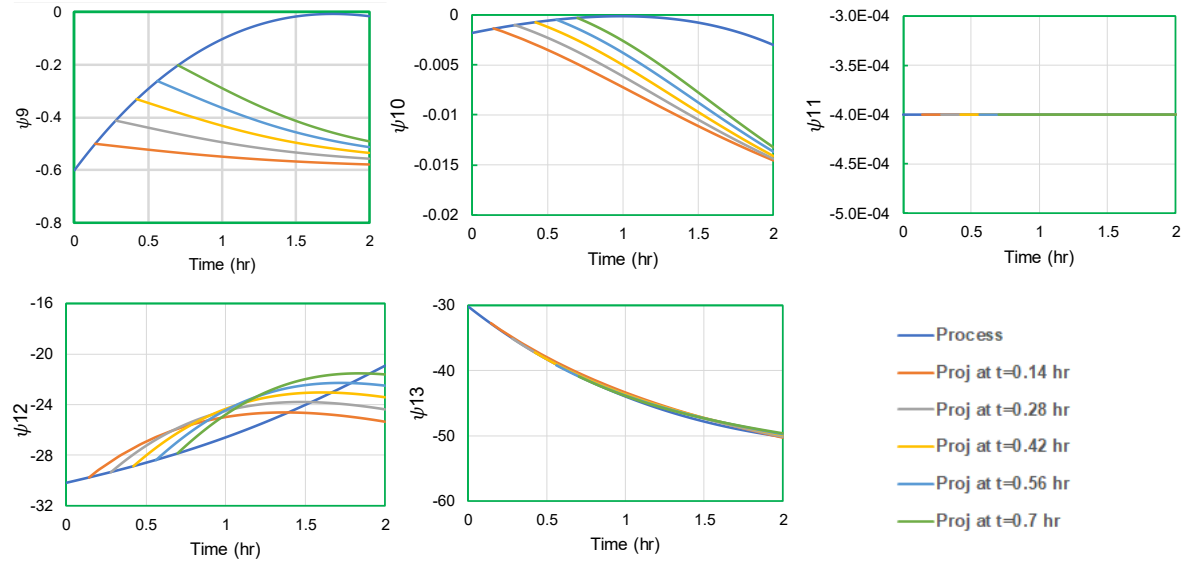

Figure 8: Real time and projected values of five constraint indices (normal operation). The projections in each plot are with the optimal MPS control action corresponding to the constraint index and the nominal values of the uncertain quantities.

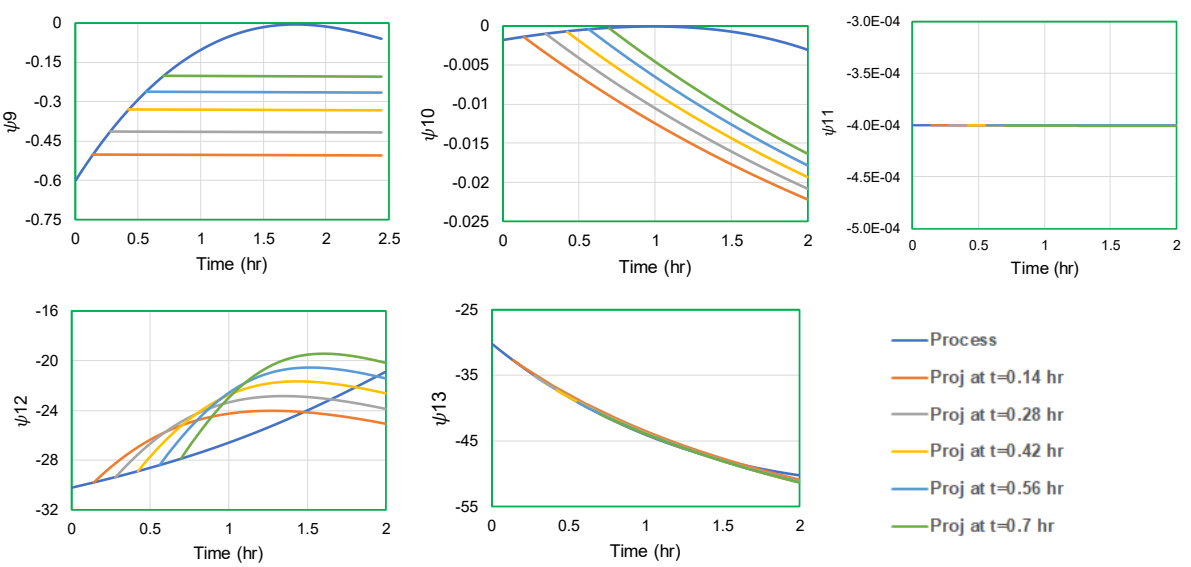

Figure 9: Real time and projected values of five constraint indices (normal operation). The projections in each plot are with the optimal MPS action corresponding to the constraint index and the worst-case values of the uncertain quantities.

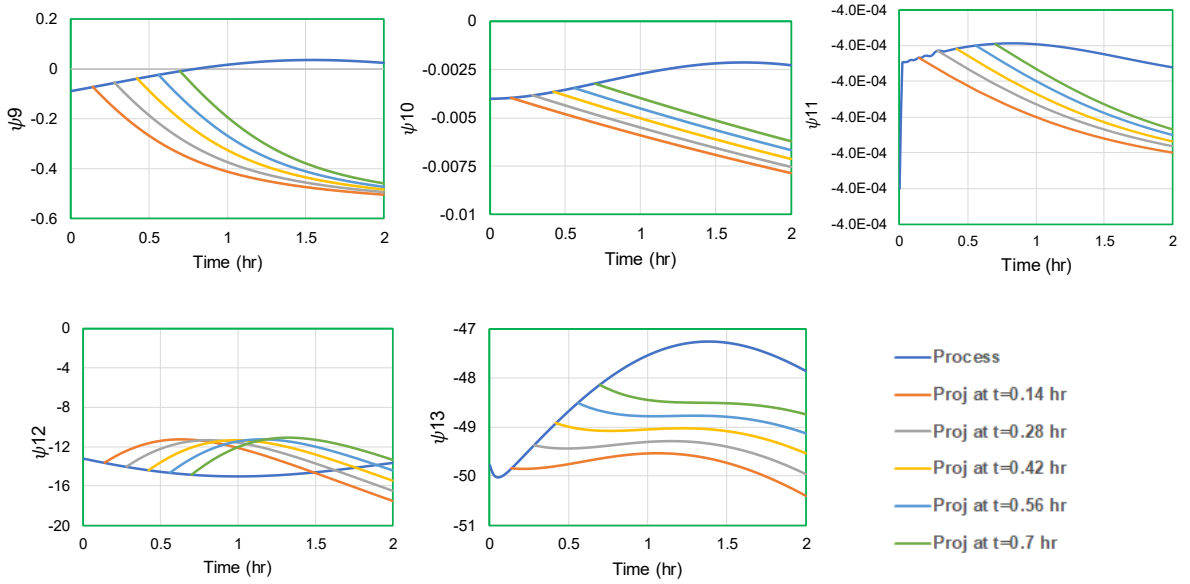

Figure 10: Real time and projected values of five constraint indices (abnormal operation). The projections in each plot are with the optimal MPS action corresponding to the constraint index and the nominal values of the uncertain quantities.

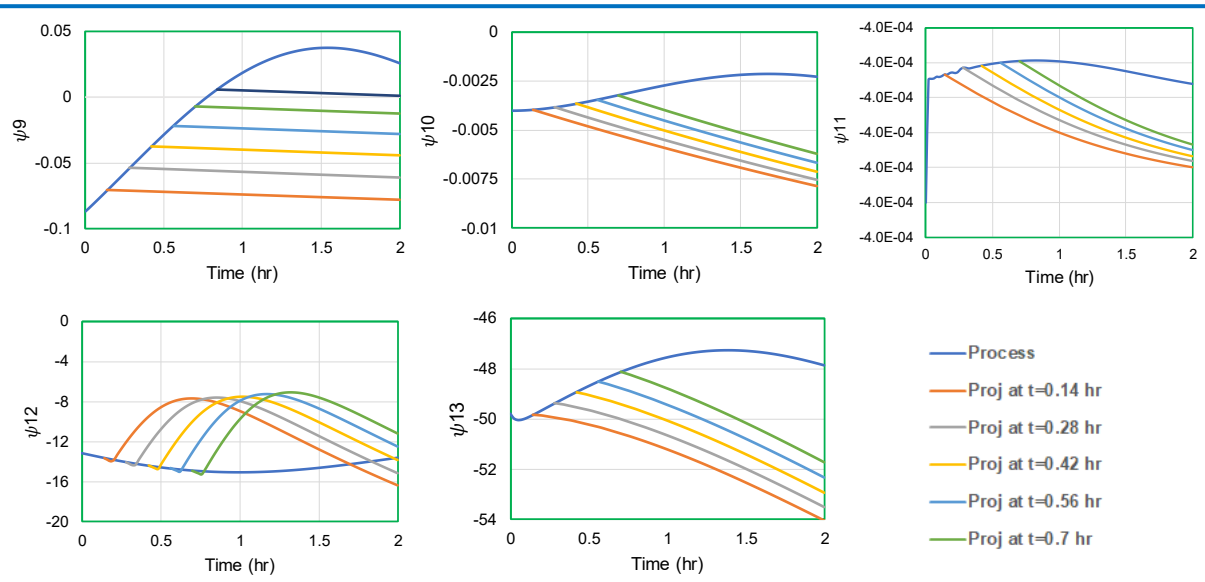

Figure 11: Real time and projected values of five constraint indices (abnormal operation). The projections in each plot are with the optimal MPS action corresponding to the constraint index and the worst-case values of the uncertain quantities.