Dynamic Risk-based Process Design and Operational Optimization via Multi-Parametric Programming

Moustafa Ali[a], Xiaoqing Cai[a,b], Faisal I. Khan[c], Efstratios N. Pistikopoulos[a,b], Yuhe Tian[d,*]

[a] *Texas A&M Energy Institute, Texas A&M University, College Station, TX 77843, United States*
[b] *Artie McFerrin Department of Chemical Engineering, Texas A&M University, College Station, TX 77843, United States*
[c] *Mary Kay O'Connor Process Safety Center, Artie McFerrin Department of Chemical Engineering, Texas A&M University, College Station, TX 77843, United States*
[d] *Department of Chemical and Biomedical Engineering, West Virginia University, Morgantown, WV 26506, United States*

Abstract

We present a dynamic risk-based process design and multi-parametric model predictive control optimization approach for real-time process safety management in process systems. A dynamic risk indicator is used to monitor process safety performance considering fault probability and severity, as an explicit function of safety-critical process variables deviation from nominal operating conditions. Process design-aware risk-based multi-parametric model predictive control strategies are then derived which offer the advantages to: (i) integrate safety-critical variable bounds as path constraints, (ii) control risk based on multivariate process dynamics under disturbances, (iii) provide model-based risk propagation trend forecast. A dynamic optimization problem is then formulated, the solution of which can yield optimal risk control actions, process design values, and/or real-time operating set points. The potential and effectiveness of the proposed approach to systematically account for interactions and trade-offs of multiple decision layers toward improving process safety and efficiency is showcased in a real-world example, the safety-critical control of a continuous stirred tank reactor at T2 Laboratories.

*Corresponding author at: Department of Chemical and Biomedical Engineering, West Virginia University, Morgantown, WV 26506, United States.
Email address: yuhe.tian@mail.wvu.edu (Yuhe Tian)

Keywords: Dynamic Risk Assessment, Fault Prognosis, Explicit Model Predictive Control, Multi-Parametric Optimization, Dynamic Optimization

1. Introduction

Process safety management (PSM) is a top priority in process operations to prevent the occurrence of accidents and the resulting severe human and financial losses with pressing impacts on the society and environment [1, 2, 3]. Process safety evaluation methods, such as hazard and operability study (HAZOP) [4] and quantitative risk analysis (QRA) [5], have been widely applied in current industrial practice which identify process hazards and add on protection layers (e.g., dike, relief valve) based on a static nominal design configuration. However, the recent burgeoning trends toward industry decarbonization, digital innovation, and advanced manufacturing have posed new challenges and opportunities to PSM with more complex, integrated, and automated plants under increasingly dynamic and volatile business, market, and supply chain environments [6]. Online process safety monitoring and smart risk management under disturbances become instrumental during daily process operations to safeguard the promises of real-time decision making for enhanced profitability, energy efficiency, and sustainability [7, 8]. Therefore, it is imperative to bridge the link between safety-critical decision making with systems-based real-time operation, which are normally performed independently without considering the interactions and trade-offs.

To support real-time PSM, quantitative process safety performance indicator is a key enabling factor which should account for the time-variant impacts of process design, operation, and disturbances. Conventional QRA approaches adapt risk as the indicator, estimated as the product of "fault probability" and "consequence severity" for a process facility [9, 10]. Some examples of process faults include reactor runaway, pipe rupture, liquid level sensor failure, etc. which can lead to consequences of fire, explosion, toxic release, etc. These approaches evaluate a steady-state snapshot of the process designs, which cannot provide a dynamic risk picture under operating condition variations. The use of generic failure data also challenges the process-specific estimation preciseness [11, 12]. Dynamic risk analysis strategies [13] are thus developed to address these gaps, the first of which was proposed by Meel and Seider in 2006 [14]. The majority of available dynamic risk analysis approaches [15, 16, 17, 18] employed Bayesian theory to determine the posterior fault probability distribution based on a prior distribution using generic historical data (e.g., database in [5]), however after any new occurrence of abnormality events or faults during operation. The consequence severity was then updated using a bow-tie, event tree, or fault tree model to capture the "cause-barrier-abnormality-consequence" relationships. The loss of intrinsic physics-based process dynamics and relationships hinders a joint decision making basis to integrate these approaches with process control and real-time optimization.

From the aspect of process control, the prevention of fault occurrence is mostly addressed by controlling safety-critical process variables (typically state variables) within their bounds. Model predictive control (MPC) has been leveraged to this purpose which was first proposed by Leveson and Stephanopoulos in 2013 [19]. However, an overall process safety performance indicator is missing which can assess the cumulative impacts of state transitions and disturbances. Research efforts have also been made to theoretically characterize a safe and stable dynamic state space operating region. Albalawi et al. [20, 21] developed a safeness index-based Lyapunov economic MPC (LEMPC) strategy, in which a safety zone was defined in the state space as a subset of the stability region determined by the Lyapunov level set. In the case of process states deviating from the safety zone, LEMPC control actions would drive states back to safety zone in finite time. Another work by Venkidasalapathy and Kravaris [22] used pertinent systems theory to calculate a set of initial states, starting from which the safety-critical constraints could be satisfied at all times despite potential safety threatening disturbances during dynamic operation. It remains a critical yet open research question on how to quantify the bounding conditions of uncertainties, for both process disturbances and modeling uncertainties, within which the above robust and safe control can be theoretically guaranteed.

To detect fault proactively at an early developing stage, Ahooyi et al. [23] developed a model-predictive safety system approach which could generate predictive alarm signals based on whether the process can satisfy its operability constraints using the most aggressive, feasible, manipulated input profiles. Bhadriraju et al. [24] applied model predictive control for fault prognosis, in which the control moving horizon estimation was utilized to predict potential fault occurrence. The forecast of fault propagation trajectory thus accounted for the process mechanistic, closed-loop control actions, and disturbances utilizing the real-time information of both measured and unmeasured process variables. In case of any potential fault occurrence during the next output horizon, alarms would be triggered ahead of time. A dynamic risk indicator was incorporated in [24]. A major limitation of these approaches lies in the tight coupling of controller output horizon with fault prognosis horizon (i.e., equal to each other). In this way, the fault prognosis capability is restricted by the online control requirement and computational power. Process design represents another key factor affecting process safety performance, which has mostly been investigated at steady state from the aspect of inherently safer design. Recent works [25, 26, 27, 28] indicated that process safety considerations could result in significant and non-intuitive design changes in the optimal process solution, compared to that driven by economics and sustainability objectives. This highlights the need to fully integrate the decision making of process design, real-time operation, and dynamic risk management across multiple time scales, despite a unified methodology is currently lacking.

To address the above challenge, in this work we develop a dynamic risk-based process design and operational optimization approach based on the PAROC (PARametric Optimization and Control) framework [29]. The remaining of the paper is organized as follows: Section 2 introduces the proposed risk-based optimization approach integrating dynamic risk analysis and multi-parametric control. Section 3 demonstrates this approach step-by-step for the safety-critical control of a real-world T2 continuous stirred tank reactor. Section 4 presents concluding remarks and future work.

2. The Risk-based Optimization Approach

2.1. Overview of the Proposed Approach

This work aims to develop a general methodology framework for risk-based process design and operational optimization. A schematic of the proposed framework is shown in Fig. 1, which features:

- A dynamic risk-based multi-parametric model predictive controller for optimal risk control at short term. The dynamic risk indicator is formulated as an explicit function of safety-critical process variable deviations during online operation.

- A dynamic optimizer at long term for safety and economics optimization. The time scale for the dynamic optimizer is independent of the controller time scale.

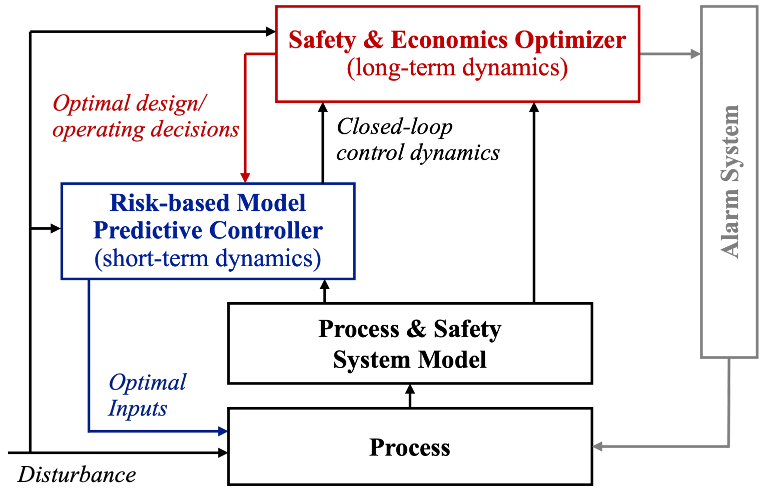


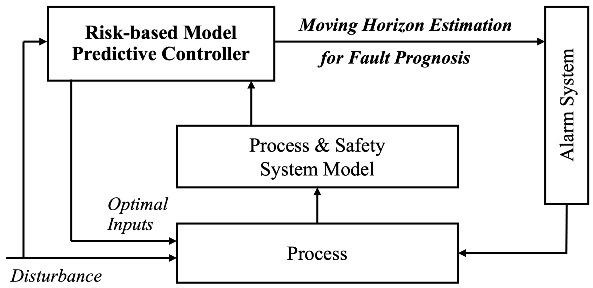
Figure 1: The integration of risk-based process design and control optimization.

Note that the decision making of controller and optimizer is fully integrated: the controller takes optimal design and/or operating decisions from the optimizer, while the optimizer is aware of the closed-loop dynamics. The potential and versatility of the framework are demonstrated through the following three classes of applications and illustrated in Fig. 2:

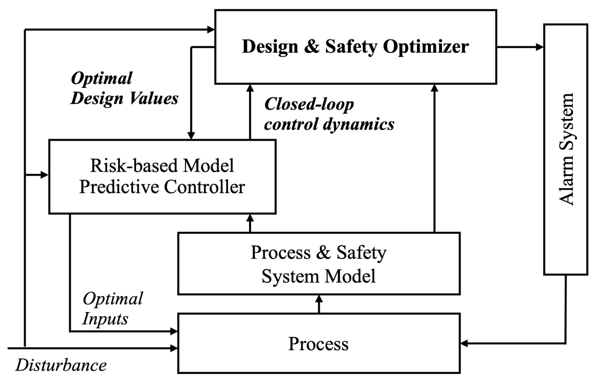
- Application 1: Model-based risk control and fault prognosis via moving horizon estimation – In this case, long-term dynamic optimizer is not used. The controller will forecast potential fault occurrence during the next output horizon and to raise alarms when necessary.

- Application 2: Simultaneous design and control optimization with dynamic risk considerations – This can be utilized to investigate interactions and trade-offs between design variables, operating variables, and safety performance metrics at the early design stage.

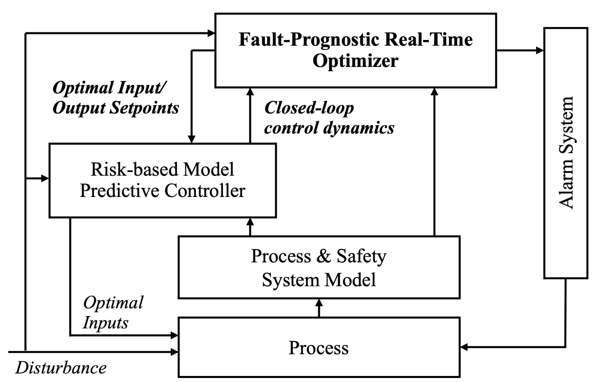
- Application 3: Integrated fault-prognostic real-time optimization and risk-based control – This can support online operation (i.e., design is fixed at this stage) to guide optimal state transitions while preserving desired process safety under disturbances. In this case, fault prognosis is achieved by the dynamic optimizer which can forecast into a longer time horizon independent of control output horizon as needed in certain processes with fast dynamics, long shutdown time, etc.



Application 1: Risk control and fault prognosis via MPC moving horizon estimation.



Application 2: Risk-based simultaneous design and control optimization.



Application 3: Fault-prognostic real-time optimization and control.

Figure 2: Applications of the general framework for risk-based design and operation.

A (mixed-integer) dynamic optimization problem (Eq. 1) is formulated to mathematically realize Fig. 1, synergizing dynamic risk analysis [30] and multi-parametric control [31]. Specifically, Eq. 1a defines the objective function for the optimizer which can account for process safety, product quality, and/or economics (e.g., design and/or operating costs). Optimization variables can include design variables and input/output set point values when applicable. Control actions at each time step are not optimization variables as they are calculated from the explicit functions of multi-parametric control law given in Eqs. 1e-f. Eqs. 1b-c describe the mechanistic dynamic model for the process and safety system (typically nonlinear). Design variables, continuous and/or discrete, can be included to consider their impact on control and risk. Eq. 1d adapts the dynamic risk indicator developed by Bao et al. [30], which quantifies risk as an explicit function of safety-critical variables deviation from nominal conditions to instantly reflect real-time process safety performance changes. This method will be detailed later in Section 2.2. Eqs. 1e-f give the multi-parametric model predictive control (mp-MPC) laws, calculated as piecewise affine functions of parameters including design variables and the risk indicator. The ability to obtain the mp-MPC control laws offline *in priori* serves as the key to connect two separate time scales (i.e., controller and optimizer) in a single dynamic optimization problem as well as to maintain tractable online computational load. The derivation of multi-parametric control laws will be detailed in Section 2.3. Eqs. 1g-i define the process operating constraints for state, input, and output variables in terms of lower and upper bounds. More generalized time-varying process operating constraints, i.e. $g(x(t), u(t), d(t)) \leq 0$, can also be incorporated when applicable following prior work [32, 33]. Eqs. 1j-k define the bounds for design and risk variables. A dual layer of process safety management is actually provided by this approach: (i) the control of dynamic risk as an overarching process safety performance indicator, (ii) the bounded operation of safety-critical variables via mp-MPC path constraints.

$$\min_{De,Y,y^R} \quad F = \int_0^\tau P(x(t), y(t), u(t), d(t), De, Y, RI(t))dt \tag{1a}$$

$$\text{s.t.} \quad dx(t)/dt = f(x(t), y(t), u(t), d(t), De, Y) \tag{1b}$$

$$y = g(x(t), u(t), d(t), De, Y), \quad Y \in \{0,1\}^q \tag{1c}$$

$$RI = s(x(t), u(t), d(t), De, d(t)) \tag{1d}$$

$$u_k = K_i\theta_k + r_i, \quad \theta_k \in CR_i = \{CR_i^A\theta \le CR_i^b\} \tag{1e}$$

$$\theta_k = [x_k, y_k, y_k^R, d_k, De, RI_k] \tag{1f}$$

$$\underline{x} \le x(t) \le \overline{x} \tag{1g}$$

$$\underline{u} \le u(t) \le \overline{u} \tag{1h}$$

$$\underline{y} \le y(t) \le \overline{y} \tag{1i}$$

$$\underline{De} \le De \le \overline{De} \tag{1j}$$

$$\underline{RI} \le RI(t) \le \overline{RI} \tag{1k}$$

where $x(t)$ are states, $u(t)$ are input variables, $y(t)$ are output variables, $d(t)$ are disturbances, Y are binary variables, De are process design variables, $RI(t)$ is dynamic risk indicator, $\theta(t)$ are parameters for mp-MPC, CR are critical regions. Subscripts k denotes discerete time step, i is index for critical regions. CR^A and CR^b are coefficient matrices to define critical regions. Superscript R denotes set point.

2.2. Dynamic Risk Modeling

In what follows we discuss the dynamic risk model proposed by Bao et al. [30] and its extension in this work to enable risk-based control. Abnormality identification is first performed for the specific process system by surveying historical incident cases and/or performing near miss studies, which aims to identify any potential faults and the associated safety-critical process variables $x(t)$. The real-time data of $x(t)$ can be either directly measurable via online monitoring or implicitly inferential via the mechanistic dynamic process model (Eqs. 1b-c). The risk indicator $RI(t)$ is defined in terms of the real-time deviation of $x(t)$ from nominal operating conditions. Two factors are considered for risk assessment, i.e. fault probability $P(x(t))$ and consequence severity $S(x(t))$ as shown in Eq. 2.

$$RI(t) = P(x(t)) \times S(x(t)) \tag{2}$$

Fault Probability

The safety-critical process variables $x(t)$ are assumed to follow statistical distributions, e.g. normal distribution characterized by the means (μ) and standard deviations (σ). The values of μ and σ are determined from the survey of industrial practice, historical cases, and open literature. μ stands for the $x(t)$ nominal operating points. $\mu \pm 3\sigma$ defines the upper and lower control limit (UCL, LCL). Statistically, 99.7% of the $x(t)$ values would fall within this three-sigma region (i.e., three-sigma rule). The fault probability $P(x(t))$ is calculated as the probability density function of normal distribution (Eq. 3), particularly stressing the fault occurrence possibility when $x(t)$ deviate away from the three-sigma region.

$$P(x(t)) = \begin{cases} \phi[\frac{x(t)-(\mu+3\sigma)}{\sigma}] = \int_{-\infty}^{x(t)} \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{[t-(\mu+3\sigma)]^2}{2\sigma^2}} \, dt, & \text{when } \; x(t) \geq \mu \\ \phi[\frac{x(t)-(\mu-3\sigma)}{\sigma}] = \int_{-\infty}^{x(t)} \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{[t-(\mu-3\sigma)]^2}{2\sigma^2}} \, dt, & \text{when } \; x(t) < \mu \end{cases} \tag{3}$$

Consequence Severity

Consequence severity $S(x(t))$ quantifies the severity of the potential hazard due to $x(t)$ deviation. An exponential function is used to calculate $S(x(t))$ as shown in Eq. 4. Importantly, the consequence severity will grow increasingly faster as the safety-critical variables deviate further away from the nominal operating point.

$$S(x(t)) = \begin{cases} 100^{\frac{x(t)-(\mu+3\sigma)}{x(t)-\mu}}, & \text{when } \; x(t) \geq \mu \\ 100^{\frac{(\mu-3\sigma)-x(t)}{\mu-x(t)}}, & \text{when } \; x(t) < \mu \end{cases} \tag{4}$$

Using Eqs. 3-4, the overall form of risk indicator $RI(t)$ follows a pseudo-exponential function. To provide a more concrete idea, Fig. 3 depicts a generic dynamic risk profile for $RI(t)$ against $x(t)$. The occurrence of a fault is defined by the risk exceeding a pre-specified threshold value determined from historical case analyses.

Major advantages of this dynamic risk model are summarized below:

- Instantaneity – Fault probability and severity data are updated instantly based on safety-critical process variable changes, which can effectively support real-time process safety monitoring

- Standardization – At $\mu \pm 3\sigma$, $P(x(t))$ is mathematically set at 0.5 and $S(x(t))$ at 1 which provide a uniform basis to benchmark various processes design and operating conditions,

- Multivariate – $RI(t)$ can capture the independent or dependent interactions between multiple process variables, e.g. via the use of multivariate joint distribution function developed in [34],

- Prediction – A linear trend risk propagation forecast is utilized in [30]. Model-based forecast will be implemented in this work taking advantage of the model predictive control and optimization capabilities.

To enable the use of linear model predictive control in Section 2.3, piecewise linearization is performed to the $RI(t)$ function as illustrated in Fig. 4. Note that the linearized $RI(t)$ values are over-estimators of the original nonlinear $RI(t)$ values. Binary variables can be introduced to reformulate the piecewise $RI(t)$ functions into a unified mathematical form as shown in Eq. 5. In addition, the piecewise functions can actually characterize distinct operating regions based on the varying risk propagation speeds. The process and risk control priorities can thus be auto-adjusted, e.g. to majorly sustain stable operation in Region 1, to start prioritizing risk control in Region 2, and to adapt increasingly aggressive risk control in Regions 3 and 4.

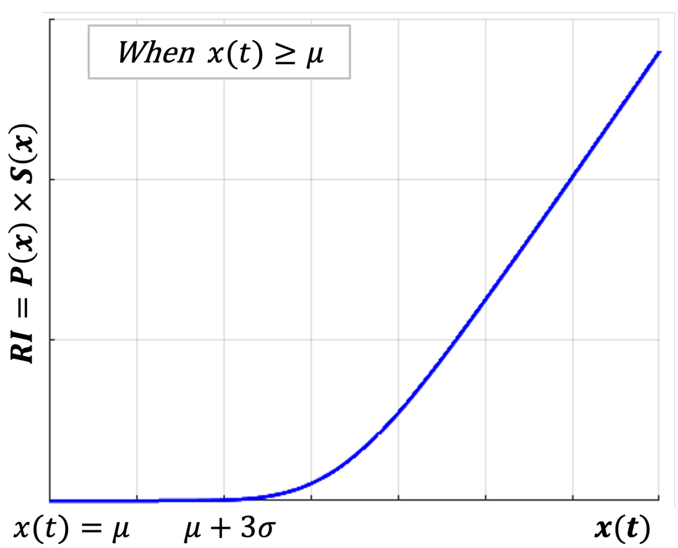


Figure 3: Dynamic risk modeling.

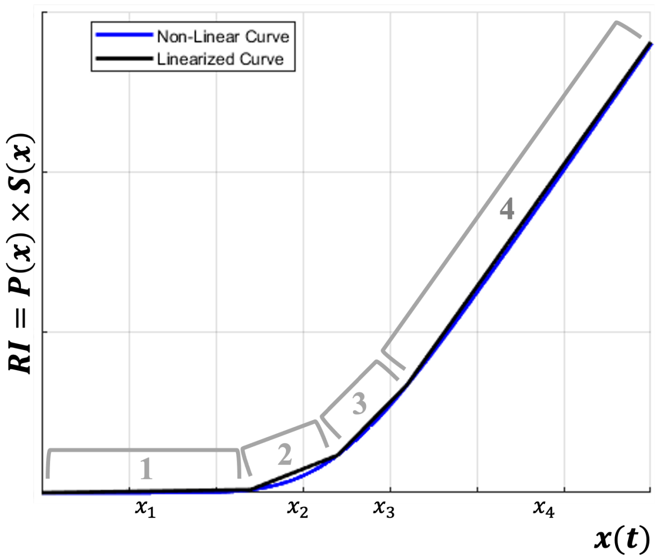


Figure 4: Piecewise linearization of dynamic risk.

$$RI(t) = \begin{cases} m_1 x(t) + b_1, & x(t) \in [\,\underline{x}_1, \overline{x}_1\,) \\ m_2 x(t) + b_2, & x(t) \in [\,\underline{x}_2, \overline{x}_2\,) \\ m_3 x(t) + b_3, & x(t) \in [\,\underline{x}_3, \overline{x}_3\,) \\ m_4 x(t) + b_4, & x(t) \in [\,\underline{x}_4, \overline{x}_4\,] \end{cases} \tag{5}$$

$$\Longleftrightarrow \qquad \begin{aligned} & RI(t) = Mx(t) + b \\ & \sum_i m_i y_i(t) = M, \quad \sum_i b_i y_i(t) = b \\ & \sum_i x_i y_i(t) = x, \qquad \sum_i y_i(t) = 1 \\ & \underline{x}_i y_i(t) \le x_i(t) \le \overline{x}_i y_i(t), \quad y_i(t) \in \{0, 1\} \\ & i \in \{1, 2, 3, 4\} \end{aligned}$$

2.3. Design-dependent Risk-based mp-MPC

The MPC problem with dynamic risk considerations is formulated as Eq. 6. Eq. 6a defines the control objective function for output/input setpoint tracking and disturbance rejection. Eqs. 6b-c represent the discrete state space model linearized from the original mechanistic process model which can be obtained using model reduction, system identification, machine learning techniques, etc. [35, 36, 37] The piecewise linearized RI functions can thus be readily integrated with the linear process state space model by treating risk as an output variable (Eqs. 6c-e). Eqs. 6f-h are the path constraints for state, input, output, design, and risk variables. It is also worth clarifying that the linearized process model and dynamic risk model are only employed here for the design of a linear model predictive controller. The closed-loop controller validation and long-term dynamic optimization are conducted against the original mechanistic-based nonlinear models (Eqs. 1b-d). Design variables De can be explicitly considered in two forms depending on the specific process system: (i) in the state space model [38, 39], and (ii) in path constraints as the upper or lower bounds of process variables. The case study in Section 3 will investigate design considerations belonging to the latter case.

$$\begin{aligned}
min_u \;\; J = \; & x_N^T P x_N + \sum_{k=1}^{OH-1} \left((y_k - y_k^R)^T QR_k \left(y_k - y_k^R \right) \right) \\
& + \sum_{k=0}^{CH-1} \left(u_k - u_k^R \right)^T R_k \left(u_k - u_k^R \right)
\end{aligned} \tag{6a}$$

$$\text{s.t.} \qquad x_{k+1} = Ax_k + Bu_k + C[d_k; De] \tag{6b}$$

$$\begin{bmatrix} y_k \\ RI_k - b \end{bmatrix} = \begin{bmatrix} D \\ M \end{bmatrix} x_k + \begin{bmatrix} E \\ 0 \end{bmatrix} u_k \tag{6c}$$

$$\sum_i m_i y_i = M \qquad \sum_i b_i y_i = b \qquad \sum_i x_i y_i = x \tag{6d}$$

$$\sum_i y_i = 1 \qquad \underline{x}_i y_i \leq x_i \leq \overline{x}_i y_i \qquad y_i \in \{0, 1\} \tag{6e}$$

$$\underline{x} \leq x_k \leq \overline{x} \qquad \underline{u} \leq u_k \leq \overline{u} \tag{6f}$$

$$\underline{y} \leq y_k \leq \overline{y} \qquad \underline{d} \leq d_k \leq \overline{d} \tag{6g}$$

$$\underline{De} \leq De \leq \overline{De} \qquad \underline{RI} \leq RI_k \leq \overline{RI} \tag{6h}$$

where P is terminal weight, QR and R are controller weights, CH and OH are respectively control and output horizons.

MPC problems can be reformulated into multi-parametric quadratic programming (mp-QP) problems as Eq. 7. More theoretical fundamentals on multi-parametric programming and its application in model predictive control can be found in the recent authored book from Pistikopoulos et al. [31]. Due to the existence of binary variables for piecewise risk functions, the design-dependent risk-based MPC formulation in Eq. 6 will finally result in a mixed-integer multi-parametric quadratic programming (mp-MIQP) problem. Decomposition-based mp-MIQP solution algorithms can be used which leverage global optimization to identify candidate binary solutions and accelerate mp-QP solution efficiency via parallel computation [40].

$$\begin{aligned} min_u \quad & f(u,\theta) = \frac{1}{2}u^T Q u + u^T H^T \theta + \theta^T Q_\theta \theta + c_u^T u + c_\theta^T \theta + c_c \\ \text{s.t.} \quad & Nu \leq b + F\theta \\ & CR^A \theta \leq CR^b \\ & u \in \mathbb{R}^n, \quad \theta \in \mathbb{R}^m, \quad Q \succ 0 \end{aligned} \tag{7}$$

The multi-parametric solution of Eq. 7 generates an optimal partition of the parameter space into a list of critical regions CR. Each critical region is dictated by a unique active set of constraints to attain optimality in Eq. 7. As shown in Eq. 8, the optimal control actions on each critical region can be explicitly expressed as an affine function of the parameter set. To the interest of this work, the parameters include states, outputs, setpoints, and disturbances as well as design variables (continuous and/or discrete) and risk indicator. Therefore, the MPC problem which typically requires online dynamic optimization can be replaced by an online function evaluation process using the optimal multi-parametric/explicit control laws generated offline *in priori*. A closed-loop validation step is performed to test the resulting mp-MPC controller for process and risk control and enhance the tuning parameters if necessary.

$$\begin{aligned} & u_k = K_i \theta_k + r_i \qquad \theta_k \in CR^i = \{CR_i^A \theta \leq CR_i^b\} \\ & \theta_k = [x_k, y_k, y_k^R, d_k, De, RI_k] \end{aligned} \tag{8}$$

3. Case Study: Exothermic CSTR at T2 Laboratory

In this section, we apply the proposed dynamic risk-based design and operational optimization approach on an exothermic CSTR process adapted from [22] based on a major process safety accident at T2 Laboratories Inc. CSTR with runaway reactions is a classical benchmark example to test safety-critical control strategies (e.g., [19, 20, 22]).

3.1. Process Description

A reactive chemical explosion accident took place at T2 Laboratories Inc. in Florida on December 19, 2007 which unfortunately resulted in 28 injuries and 4 fatalities [41]. The T2 process produced methylcyclopentadienyl manganese tricarbonyl, an Ecotane brand gasoline additive. A runaway chemical reaction occurred during the first production step in a 2500-gallon batch reactor. The two exothermic reactions involved in this batch reactor are given below. The second reaction rate becomes significant only at elevated temperature. Due to the inadequate cooling system, the pressure and temperature within the reactor increased uncontrollably which eventually ignited hydrogen as a major reaction product and other flammable byproducts.

<u>Reaction 1:</u> Methylcyclopentadiene (A) + Sodium (B) $\xrightarrow{Diglyme(S)}$ Sodium Methylcyclopentadiene (C) + Hydrogen (D)

<u>Reaction 2:</u> Diglyme (S) $\xrightarrow{Sodium(B)}$ Hydrogen (D) + Byproduct

In this work, we investigate the use of a CSTR at similar conditions to the original T2 batch reactor as per [22]. The process can be conceptualized as Fig. 5. There are two feed streams to the CSTR, one consisting of reactant A in solvent S and the other of reactant B. To initiate the reactions, the feed streams are preheated before entering the reactor. Reactor temperature T is selected as the safety-critical process variable, which should be controlled at a setpoint (e.g., 460 K) despite possible fluctuations of feed inlet temperature T_0. Cooling is provided via an evaporating water jacket, the heat transfer coefficient U of which can be adjusted via cooling water flow rate m_c. For simplification, U is considered as the manipulated variable in this study. The maximum value of heat transfer coefficient U_{max} is then utilized as the cooling system design parameter. The high risk region is defined as $T \geq 480K$, in which thermal runaway is at higher probability to occur due to the rapidly

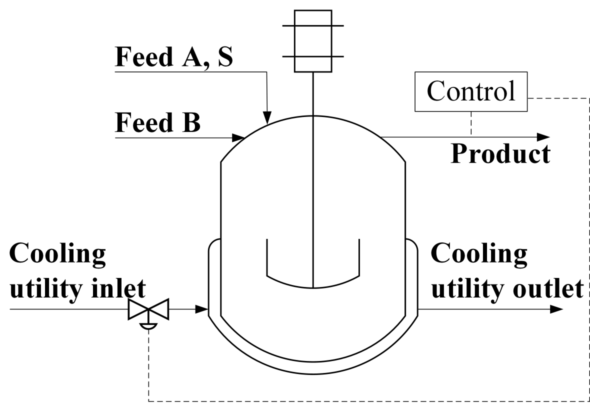


Figure 5: The T2 CSTR process.

increasing reaction rates (particularly of reaction 2). The research objectives of this case study are to:

1. Control the risk at a desired level under disturbances.

2. If thermal runaway cannot be prevented, attenuate the risk propagation speed and consequence severity while raising the alarm ahead of fault occurrence time for operator response (e.g., $\geq$ 10 minutes).

3. Identify the optimal design configuration and closed-loop control actions under disturbances with constrained dynamic risk.

4. Achieve optimal and safe operation via real-time optimization with process-tailored fault prognosis horizon.

In the second objective, the 10-min fault prognosis horizon is used as an indicative minimum allowable operator response time based on industrial practice [42]. The underlying assumption is that, if alarm can be raised 10 minutes before actual fault occurrence, operators can prudently perform the shutdown. Longer time horizon can also be used (e.g., $\geq$ 20 minutes) to enable ample time for response and/or to tailor process-specific requirements [43]. Though the proposed methodology framework is generally applicable, it is a trade-off decision on how to optimally determine the fault prognosis horizon (and also the risk threshold to raise alarm). A longer fault prognosis horizon enables more time for operator response while may result in more conservative control actions based on estimated disturbances and process conditions in future time steps.

3.2. T2 CSTR Risk-based Optimization

In what follows, we present the step-by-step application of the proposed approach to this T2 CSTR case study. The step-wise procedure is summarized in Fig. 6 based on the PAROC framework [29].

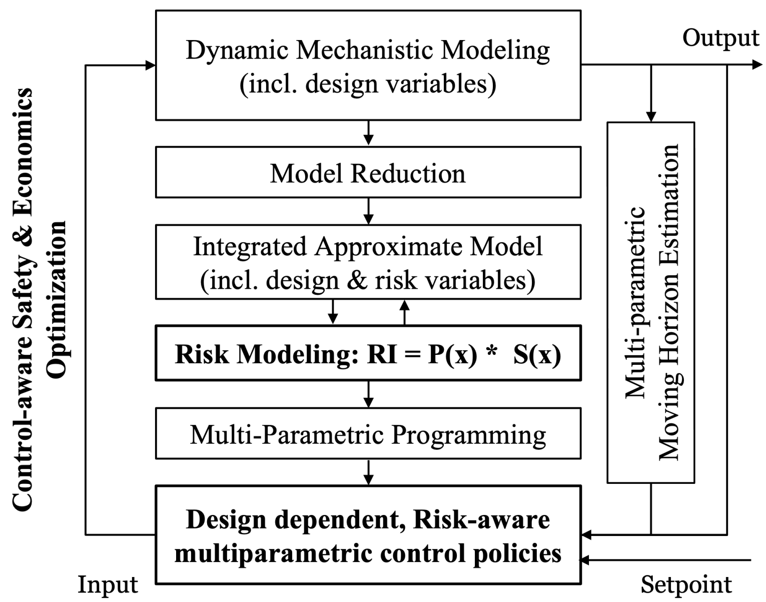


Figure 6: The step-wise procedure for controller and optimizer implementation.

3.2.1. Mechanistic Dynamic Modeling

We first develop a mechanistic dynamic model for the process (and safety) system of interest. An ideal CSTR with constant reactor volume is assumed to be in use. The nonlinear dynamic model is given in Eq. 9. Eqs. 9a-c describe the dynamic mass balances for reactants A, B, and S. Eq. 9d describes the dynamic energy balance in reactor. A list of the major process variables are summarized in Table 9. The kinetics and process parameter values are provided in Appendix A.

$$\frac{dC_A(t)}{dt} = \frac{F_{A,in}}{V} - \frac{q_{out}}{V}C_A(t) - k_1(T(t))C_A(t)C_B(t) \tag{9a}$$

$$\frac{dC_B(t)}{dt} = \frac{F_{B,in}}{V} - \frac{q_{out}}{V}C_B(t) - k_1(T(t))C_A(t)C_B(t) \tag{9b}$$

$$\frac{dC_S(t)}{dt} = \frac{F_{S,in}}{V} - \frac{q_{out}}{V} C_S(t) - k_2(t) C_S(t) \tag{9c}$$

$$\frac{dT(t)}{dt} = \frac{q_{out}}{V}(T_{in}(t) - T(t)) + \frac{\sum(-\Delta H_k) r_k(t)}{\rho c_p} - \frac{U A_x (T(t) - T_c)}{\rho c_p V} \tag{9d}$$

Table 1: List of CSTR process variables.

Symbol	Definition	Variable(s)	Physical Description	Unit
$x(t)$	States	C_A, C_B, C_S	Concentrations	mol/l
		T	Reactor temperature	K
$u(t)$	Input	U	Heat transfer coefficient	$\mathrm{kJ/(K \cdot h \cdot m^2)}$
$d(t)$	Disturbance	T_0	Feed inlet temperature	K
De	Design	U_{max}	Maximum heat transfer coefficient	$\mathrm{kJ/(K \cdot h \cdot m^2)}$

The mechanistic dynamic model is built in both MATLAB® and gPROMS® ModelBuilder in preparation for the next step analyses. An open-loop simulation is performed to study reactor dynamics particularly regarding thermal runaway risk. A disturbance step change of $\Delta T_{in} = 25$ K is introduced at $t = 0$ which can be resulted by a severe malfunction of the feed preheater. As shown in Fig. 7, reactor temperature increases to the high risk region after ~ 9 hours ($T \geq 480$ K), following which thermal runaway occurs.

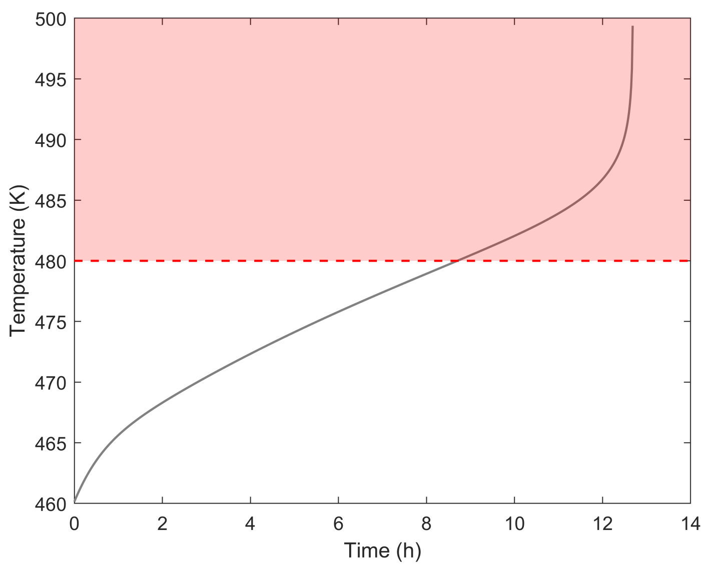


Figure 7: T2 CSTR open-loop simulation.

3.2.2. Model Reduction

The nonlinear CSTR model is then linearized around steady state using Jacobian matrices calculated by MATLAB® jacobian function. A discrete linear state space model is obtained as given in Eq. 10.

$$\begin{bmatrix} \overline{C}_A \\ \overline{C}_B \\ \overline{C}_S \\ \overline{T} \end{bmatrix}_{k+1} = A \begin{bmatrix} \overline{C}_A \\ \overline{C}_B \\ \overline{C}_S \\ \overline{T} \end{bmatrix}_{k} + B\overline{U}_k + C\overline{T}_{in,k}, \quad T_s = 1 \text{ min} \tag{10}$$

where the deviation variables are defined as $\overline{X} = X - X_{ss}$. The coefficient matrix values are:

$$A = \begin{bmatrix} 0.9506 & -0.0047 & 0 & -0.0003 \\ -0.0484 & 0.9943 & 0 & -0.0003 \\ 0 & 0 & 0.9990 & -1.5740 \times 10^{-6} \\ 0.6970 & 0.0678 & 0.0002 & 1.0030 \end{bmatrix}$$

$$B = \begin{bmatrix} 0 \\ 0 \\ 0 \\ -0.0007 \end{bmatrix} \qquad C = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0.0010 \end{bmatrix}$$

The linearized CSTR model is validated against the original nonlinear model in Fig. 8. The two models match well up to $T \approx 480$ K while the linearized model cannot capture the temperature surge in high risk region. This also highlights the importance to apply the original nonlinear model for closed-loop control validation in Section 3.2.4 and dynamic optimization in Section 3.2.5.

In case that significant deviations exist between the Jacobian-based linearization model and the original nonlinear model, linear state space model can be generated using other techniques such as model reduction, system identification, and machine learning [35, 36, 37]. Moreover, in the current work, the approximated model is generated by sampling over the entire expected operating region. Strategies have also been developed in recent integrated design and control literature which aimed to approximate and validate the overall dynamic optimization problem against a specific operating point (e.g., worst-case variability point) using trust-region approach [44], back-off approach [45, 46], etc. Online model updating and nonlinear model pre-

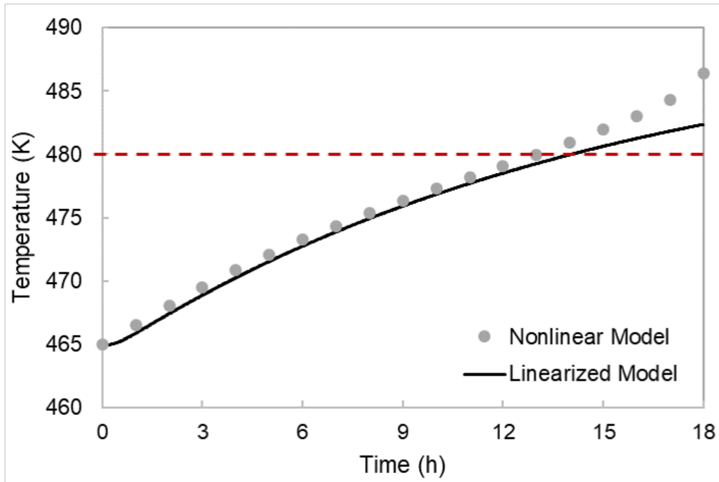


Figure 8: Comparison of linearized vs. nonlinear CSTR model.

dictive control provide alternative ways to overcome model approximation errors, which are briefly discussed in the concluding remarks section.

3.2.3. Dynamic Risk Modeling

We proceed to model the dynamic risk as a function of reactor temperature, namely the safety-critical variable for this T2 CSTR process. Following the methodology presented in Section 2.2, the reactor temperature is assumed to follow normal distribution. The nominal operating temperature is adapted at $\mu = 460$ K as per open literature data. The standard deviation is set at $\sigma = 5$ K which gives the upper control limit as $UCL = \mu + 3\sigma = 475$ K. The risk threshold is defined at $RI \geq 2.82$ according to the high risk region at $T \geq 480$ K. In other words, if the risk value exceeds 2.82 during operation, a fault occurs. The dynamic risk can thus be quantified using Eqs. 3 and 4 (only $x \geq \mu$ is of interest). To linearize the risk model as per Fig. 4, four piecewise affine functions are identified with the expressions listed in Eq. 11.

$$\overline{RI}_k = RI_k - b = M \begin{bmatrix} \overline{C}_A \\ \overline{C}_B \\ \overline{C}_S \\ \overline{T} \end{bmatrix}_k \tag{11}$$

$$M = \begin{bmatrix} 0 \\ 0 \\ 0 \\ m \end{bmatrix}^T, m = \begin{cases} 0.0078, & T \in [460, 472] \\ 0.2147, & T \in [472, 477] \\ 0.5496, & T \in [477, 481] \\ 0.7629, & T \in [481, 495] \end{cases}, b = \begin{cases} -0.1165, & T \in [460, 472] \\ -0.7374, & T \in [472, 477] \\ -0.0662, & T \in [477, 481] \\ 1.2120, & T \in [481, 495] \end{cases}$$

Up to this step, an integrated linear state space model has been obtained for dynamic process and risk modeling, which will be used for the next step controller design:

$$\begin{aligned} \begin{bmatrix} \overline{C}_A \\ \overline{C}_B \\ \overline{C}_S \\ \overline{T} \end{bmatrix}_{k+1} &= A \begin{bmatrix} \overline{C}_A \\ \overline{C}_B \\ \overline{C}_S \\ \overline{T} \end{bmatrix}_k + B\overline{U}_k + C\overline{T}_{in,k} \\ \overline{RI}_k &= M \begin{bmatrix} \overline{C}_A \\ \overline{C}_B \\ \overline{C}_S \\ \overline{T} \end{bmatrix}_k \qquad T_s = 1 \text{ min} \end{aligned} \tag{12}$$

3.2.4. Design-dependent Risk-based Multi-Parametric Controller design

A mp-MPC problem is formulated as per Eq. 6 using the above integrated linear state space model. Risk is incorporated as the output variable and bounded via the path constraints. The cooling system design variable U_{max} is considered through the path constraints $\underline{U} \leq U \leq U_{max}$. This step is implemented in MATLAB® using the POP Toolbox [47].

We first investigate dynamic risk management solely with mp-MPC and fault prognosis relying on moving horizon estimation. An output horizon of $OH = 10$ is selected which allows a 10-min risk forecast horizon (or fault prognosis). In other words, the controller computes the optimal action at the current time point by optimizing the disturbance rejection performance over the next 10 min. However, if the risk is projected to exceed the threshold value ($RI \geq 2.82$) during the next output horizon, an alarm will be raised around 10 minutes earlier to alert the operator. This will enable the operator to prudently plan for abnormality response or process shutdown. The mp-

MPC tuning parameters are listed in Table 2 and path constraints in Table 3 (in terms of deviation variables).

Since only 4 binary variables are involved in this case study while being mutually exclusive, we solve the resulting mp-MIQP problem by enumerating all the four possible integer solutions. A superset of four mp-QP solution maps is generated and the solution of mp-MIQP is determined by searching through the mp-QP maps (illustrated in Fig. B1). Each mp-QP problem is solved to have 59 critical regions with 8 parameters. The parameter set includes $\overline{C}_A$, $\overline{C}_B$, $\overline{C}_S$, and $\overline{T}$ as 4 state variables, $\overline{RI}$ as output variable, $\overline{RI}^R$ setpoint, $\overline{T}_{in}$ as disturbance, and $\overline{U}_{max}$ as design variable.

Table 2: mp-MPC tuning parameters.

OH	CH	QR	R
10	1	10^4	10^{-6}

Table 3: mp-MPC path constraints.

	$\overline{C}_A$, $\overline{C}_B$, $\overline{C}_S$, $\overline{T}$	$\overline{RI}$	$\overline{U}$	$\overline{T}_{in}$
Max	10, 10, 10, 25	25	$\overline{U}_{max}{}^*$	100
Min	-10, -10, -10, -15	-3	-55*	-20

* $\overline{U}_{max}$ is the design variable

** CSTR heating duty is also available ($U < 0$)

The resulting mp-MPC controller is applied to the nonlinear CSTR and risk model for closed-loop control using the following three scenarios:

- Scenario 1: Control at low risk level

The CSTR initial states are at $C_A = 0.4$ mol/l, $C_B = 1.5$ mol/l, $C_S = 2.5$ mol/l, and $T = 460$ K. A step change of the disturbance is introduced at $t = 0$ with $\Delta T_{in} = 25K$. As shown in Fig. 9, the open-loop process (i.e., without controller) enters the high risk region after approximately 9 hours. On the other hand, the risk-based multi-parametric controller can effectively control the CSTR at low risk level ($RI \approx 0.00175$) with a set point at $RI^R = 0$.

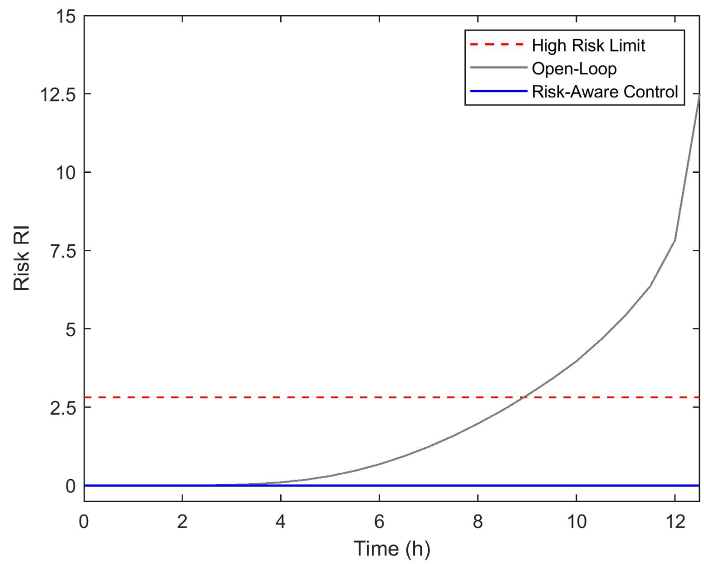


Figure 9: Scenario 1 – Closed-loop control at low risk level.

- Scenario 2: Control at medium risk level

Sometimes it may be desired to operate the reactor at higher temperatures despite the increase of risk, for example to attain higher productivity. Given this, the controller is tested against a risk set point of $RI^R = 0.74$ which lies between the upper control limit and the high risk limit. Fig. 10 shows the closed-loop results. The controller adapts an initial heating step to rapidly increase the reactor temperature to the desired temperature setpoint but is able to stabilize the process afterwards in prevention of further risk surge.

- Scenario 3: Fault prognosis and alarm raising

In certain cases, the process risk cannot be prevented from entering the high risk region due to notably large disturbances, insufficient cooling water availability, or more stringent risk limit. With the mp-MPC output horizon as 10 min, a ten-minute fault prognosis horizon can be achieved using model-based risk forecast. An example is shown in Fig. 11. At t = 11.13 h, the mp-MPC forecasts that the risk will enter the high risk region in the next 10 minutes. An alarm is thus raised to alert the operator. At t = 11.35 h, the real-time risk value reaches the high risk region, i.e. a fault happens. The 13.2 minutes between alarming raising and fault occurrence will be crucial for the operator to take response actions in a proactive manner. Importantly, the controller can continue mitigating the risk at the same time, to significantly reduce its propagation speed and fault severity compared to open-loop operation.

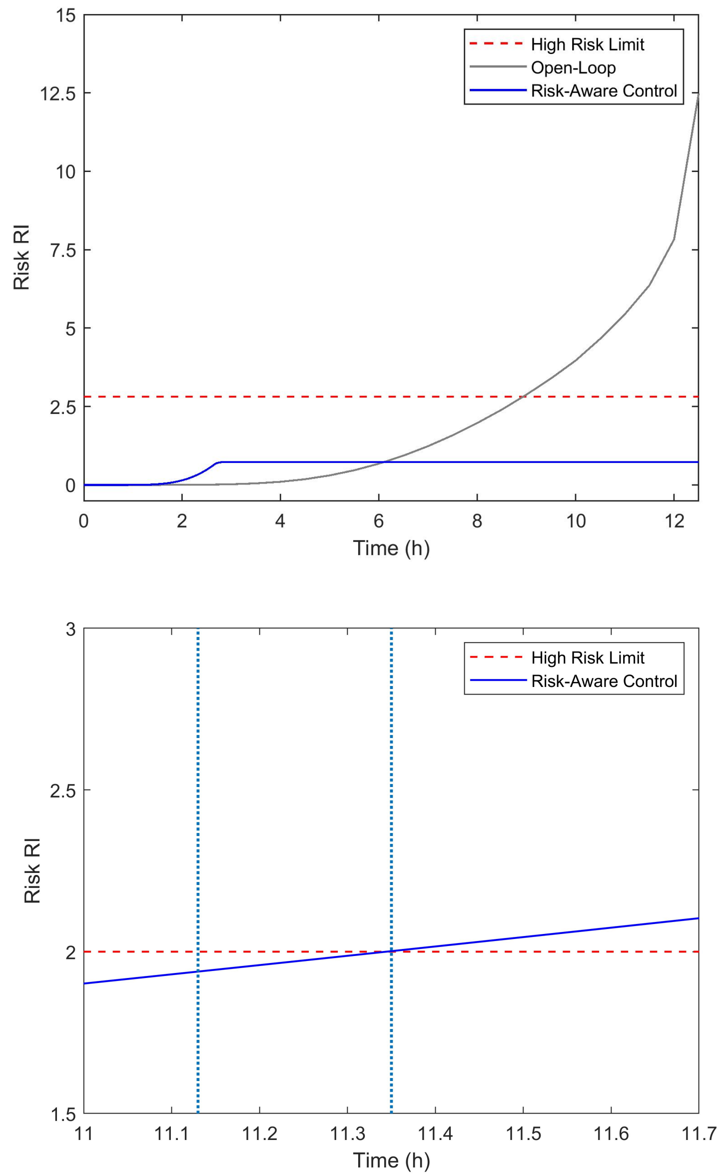


Figure 11: Scenario 3 – Control-aware fault prognosis and alarm raising. $t = 11.13$ h: alarm raised, $t = 11.35$ h: fault happens

We have demonstrated the proposed approach for dynamic risk management and fault prognosis exclusively via predictive control, which restricts the risk forecast horizon equal to control output horizon. In certain process systems such as with very fast dynamics, it is challenging to achieve a sufficient fault prognosis horizon for the operator from process safety management aspect. In Section 3.2.5, we will augment the risk-based controller with a control-aware dynamic optimizer to empower decision making across distinct time scales. This will also extends the strategy for integrated design, economics, and safety optimization. To relax the control decision horizon, in what follows we will use a new mp-MPC controller with $OH = 2$ and $CH = 1$. Closed-loop validations are performed which have justified the risk control efficacy under Scenarios 1 and 2. The corresponding explicit control laws are included in Appendix B.

3.2.5. Control-aware Safety and Economics Optimization

We investigate two classes of applications for the integration of risk-based mp-MPC with dynamic optimization as per Fig. 1: (i) simultaneous risk-based process design and control optimization, (ii) fault-prognostic real-time optimization and control. For this specific case study, the economic considerations comprise the process design and operating cost (i.e., utility cost). As the operation of this exothermic CSTR is considered at high temperature under potential runaway risk, we assume that the product specification for C (the only liquid product) will always be satisfied when reactor temperature is above 460 K. In certain other case studies, off-spec products may be generated due to insufficient control far from the set point (e.g., if higher temperature results in less productivity or selectivity) while it takes time for risk to propagate to high limit. Economic losses during this off-spec period can be readily incorporated to the objective function.

This step is implemented in gPROMS® ModelBuilder using CVP_SS as the dynamic optimization solver. The multi-parametric control laws derived from Section 3.2.4 are exported from MATLAB® and embedded in gPROMS®.

- Application 1: Simultaneous Risk-based Design and Control

The control-aware dynamic optimization formulation for this T2 CSTR case study is given in Eq. 13. In the objective function, $\int_0^\tau U\, dt/\tau$ quantifies the average operating cost given that U is a pseudo-linear function of cooling water flowrate. WU_{max} indicates the design cost. U_{max} is considered as a *time-invariant* design variable. W is a weighting factor to balance the operating and design cost, which currently takes the value of 1. The dynamic optimization is performed under a worst-case scenario (e.g., with step change $\Delta T_{in} = 25$ K) over $\tau = 100$ h to ensure the risk dynamics reach a new steady state (though much longer than enough).

U_{max} is treated as the only degree of freedom for this optimization problem. Note that the multi-parametric control laws generated offline will compute the optimal control actions based on the real-time values of states, disturbances, risk indicator, and design variable. In other words, the mp-MPC control laws are designed a priori but the optimal control actions are calculated in real time and affected by the design variable (see Appendix B for an example of mp-MPC explicit control laws). The values of process initial states and risk set point remain same with the above control studies. By varying the risk tolerance at the end point of τ, a list of optimal cost objective values are obtained with the associated design variable values. For example, to achieve the end-point $RI \leq 0.00175$ (i.e., low risk level control in Scenario 1), the optimal design variable U_{max} is 48.2 kJ/(K · h · m^2) compared to the nominal value used earlier as 55 kJ/(K · h · m^2). Fig. 12 quantitatively depicts this trade-off to assist decision making for the optimal design and operation of safety-critical process systems.

$$
\begin{array}{lll}
min & F = \int_0^\tau U(t)\,dt/\tau + WU_{max} & \text{Cost-objective function} \\
\text{s.t.} & dx(t)/dt = f(x(t), u(t), d(t), De, Y) & \text{Nonlinear CSTR model (Eq. 9)} \\
 & RI = s(x(t), u(t), d(t), De, Y) & \text{Nonlinear risk model (Eqs. 2-4)} \\
 & u_k = K_i\theta_k + r_i & \text{Multi-parametric control laws} \\
 & \theta_k \in CR_i = \{CR_i^A\theta \leq CR_i^b\} & (OH = 2,\ CH = 1) \\
 & \theta_k = [x_k, y_k, y_k^R, d_k, De, RI_k] & \text{(Section 3.2.4, Eq. B1)} \\
 & \underline{x} \leq x(t) \leq \overline{x} & \text{Below are path constraints} \\
 & \underline{u} \leq u(t) \leq U_{max}, \quad \underline{y} \leq y(t) \leq \overline{y} & \\
 & \underline{De} \leq De \leq \overline{De}, \quad \underline{RI} \leq RI(t) \leq \overline{RI} &
\end{array}
\tag{13}
$$

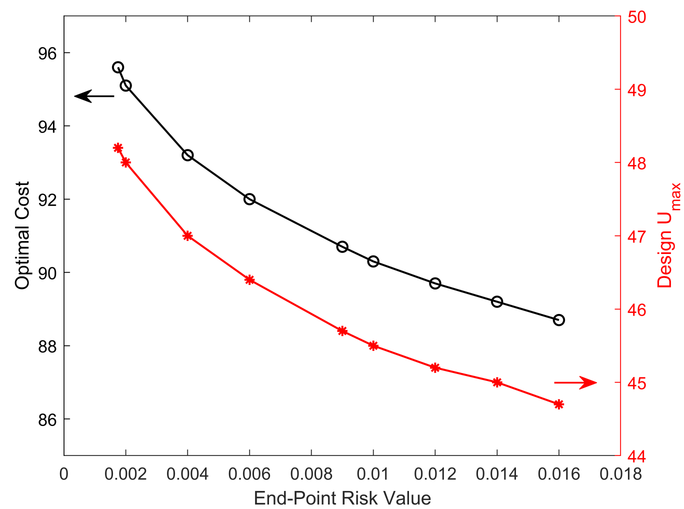


Figure 12: Optimal cost versus end-point risk limit.

- Application 2: Fault-Prognostic Real-Time Optimization and Control

Herein, we consider U_{max} as a *time-variant* variable which can be adjusted in real time. In this context, the dynamic optimizer in Eq. 13 takes the role of real-time optimization to determine the cost-optimal U_{max} value simultaneously with dynamic risk management and fault prognosis. If the risk is predicted to exceed the threshold, an alarm will be raised in advance. It is worth highlighting that the dynamic optimizer is aware of the closed-loop process, risk, and control dynamics. As illustrated in Fig. 13, the fault-prognostic optimizer forecast horizon τ is selected to be 30 min as an example. The resulting optimal U_{max} is then passed to the risk-aware controller. However, when applicable, the dynamic optimizer tends to strictly meet the end-point risk tolerance in exchange for lower design and operating cost which will then challenge the risk control in the next 30 min. Given this, the fault-prognostic optimizer is set to be activated in every 20 min to start the next round economics and safety optimization. Note that the characteristic times can be flexibly selected tailored to the process-specific need. For consistency, we again test the strategy to operate this T2 CSTR under a step change of $\Delta T_{in} = 25$ K with $RI \leq 0.00175$ at end of every optimizer forecast horizon τ. The results are shown in Fig. 14, in which the real-time U_{max} values can effectively guide the controller for dynamic risk management with cost-optimality at each step.

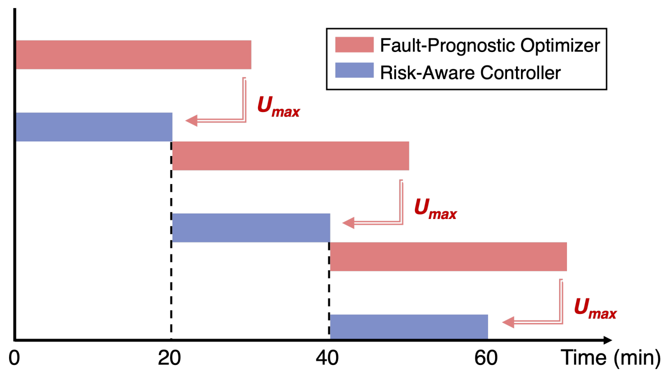


Figure 13: Integration scheme for fault-prognostic optimizer and risk-aware controller.

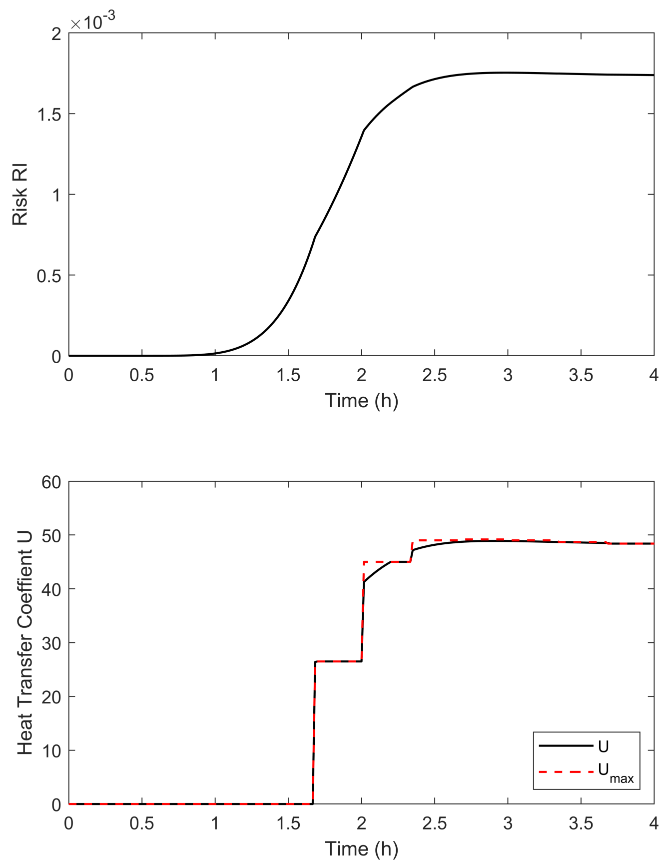


Figure 14: Real-time optimization of cooling water consumption.

4. Concluding Remarks

We have introduced a general framework for process design and operational optimization with online process safety monitoring and proactive risk management. A model-based risk control strategy is developed via multi-parametric programming, which also enables fault prognosis and alarm management via moving horizon estimation. The risk-based control is further augmented with dynamic optimization to address optimal decision making across multiple decision layers with potentially distinct characteristic time scales (i.e., design, real-time optimization, control, and fault prognosis). The efficacy and applicability of the approach has been demonstrated on the safety-critical operation of an exothermic CSTR at T2 Laboratory, Inc.

The current work utilizes linear model predictive control which inevitably introduces model approximation errors against the original nonlinear mechanistic model. Robust (multi-parametric) model predictive control provides a classical solution to address bounded errors due to model approximation [48]. Online model updating offers another option which can leverage Bayesian approach [49], neural network [50, 51], and other machine learning techniques [52] to achieve reliable model predictive control by continuously learning process mechanistic. More recently, nonlinear model predictive control (NMPC) has gained increasing momentum with significant algorithmic improvement to speed up computational times and enhanced fundamental understanding on stability and robustness properties [53, 54, 55]. NMPC strategies have been developed for highly nonlinear processes [56], economic MPC [57, 58], and integration with design or higher level operational decisions (e.g., real-time optimization [59, 60], simultaneous design and control [44]). Multi-parametric programming has also been extended to obtain explicit NMPC laws in prior work, e.g. for convex quadratically constrained control problems [61] and for generalized nonlinear process control based on balancing of empirical gramians [36]. Ongoing work is addressing the comparison of multi-parametric linear control versus nonlinear control particularly in the safety-critical chemical processes.

Acknowledgement

M. Ali, X. Cai, E. N. Pistikopoulos, F. I. Khan acknowledge financial support from Texas A&M Energy Institute and Mary Kay O'Connor Process Safety Center. Y. Tian acknowledge start-up funds from Department of Chemical and Biomedical Engineering at West Virginia University.

Appendix A: T2 CSTR Reaction Kinetics and Process Parameters

The reaction rate expressions and CSTR reactor parameter definitions are given below adapted from [22].

<u>Reaction 1:</u> $r_1 = -k_1 C_A C_B$, where $k_1 = k_{10} exp(-\frac{E_1}{RT})$

<u>Reaction 2:</u> $r_2 = -k_2 C_S$, where $k_2 = k_{20} exp(-\frac{E_2}{RT})$

Table A1: List of CSTR process parameters.

Variable	Description	Value	Unit
$F_{A,in}$	Feed flowrate (A)	1050	mol/h
$F_{S,in}$	Feed flowrate (S)	525	mol/h
$F_{B,in}$	Feed flowrate (B)	1250	mol/h
ρ_{AS}	Feed molar density (AS)	7.33	mol/l
ρ_B	Feed molar density (B)	36	mol/l
ρ	Mixture molar density in CSTR	7.31	mol/l
k_{10}	Rate constant (reaction 1)	4×10^{14}	l/mol
k_{20}	Rate constant (reaction 2)	1×10^{84}	1/h
E_1	Activation energy (reaction 1)	1.28×10^5	J/mol/K
E_2	Activation energy (reaction 2)	8×10^5	J/mol/K
ΔH_1	Heat of reaction 1	-45400	J/(mol B)
ΔH_2	Heat of reaction 2	-3.2×10^5	J/(mol S)
V	Reactor volume	4000	l
C_p	Average specific heat	430.91	J/mol/K
T_c	Coolant temperature	373	K
A_x	Heat transfer area	5.3	m^2

Appendix B: Multi-Parametric/Explicit Control Laws

This appendix presents more detail for the design-dependent risk-aware mp-MPC with $OH = 2$, $CH = 1$ (Section 3.2.4). The resulting mp-MIQP problem is solved by enumerating 4 mp-QP problems, which are partitioned as per the temperature ranges for RI piecewise linearization. Namely, T respectively in [460, 472], [472, 477], [477, 481], and [481, 495] (Eq. 11). The conceptualization is illustrated in Fig. B1. Each mp-QP problem is solved to have 11 critical regions with 8 parameters.

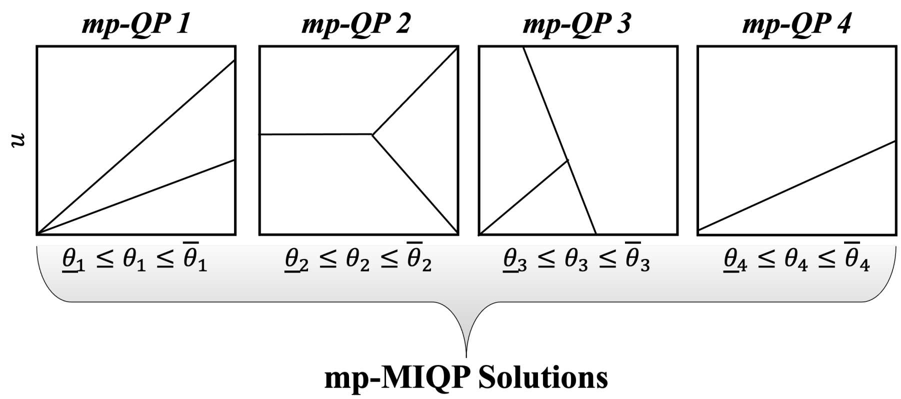


Figure B1: mp-MIQP solutions as a superset of mp-QPs.

To provide a more concrete idea on the form of multi-parametric/explicit control laws, the optimal control solution on Critical Region 1 of the mp-QP problem for $T \in [460, 472]$ is listed below. Fig. B2 further gives a geometrical view of critical regions at the CSTR initial states. θ_5 is the deviation variable for *disturbance* (i.e., $\overline{T}_{in}$) and θ_6 is the deviation variable for *risk* (i.e., $\overline{RI}$).

Critical Region 1 (CR01):

- $\theta = [\overline{C}_A, \overline{C}_B, \overline{C}_S, \overline{T}, \overline{T}_{in}, \overline{RI}^R, \overline{U}_{max}]$
- $u = K_1\theta + r_1$
  $K_1 = [130.34,\ 12.68,\ 0.033,\ 0.56,\ 0.19,\ 2.41 \times 10^4,\ -2.41 \times 10^4,\ 0]$
  $r_1 = 0$
- $CR_1 = \{CR_1^A\theta \leq CR_1^b\}$
  Constraints for upper and lower bounds of parameters are skipped for brevity, but can be found in Table 3.

$$CR_1^A = \begin{bmatrix} 0.0247 & 0.0024 & 6.3e-6 & 0.041 & 3.7e-5 & -0.7063 & 0.7063 & 0 \\ -0.0949 & 0.9955 & -4.4e-8 & -0.0006 & -2.6e-7 & 0.0049 & -0.0049 & 0 \\ 0.024 & 0.0023 & 6.3e-6 & 0.0206 & 3.7e-5 & -0.7068 & 0.7068 & 0 \\ -0.0247 & -0.0024 & -6.3e-6 & -0.041 & -3.7e-5 & 0.7063 & -0.7063 & 0 \\ 0.0949 & -0.9955 & 4.4e-8 & 0.0006 & 2.6e-7 & -0.0049 & 0.0049 & 0 \\ -0.024 & -0.0023 & -6.3e-6 & -0.0206 & -3.7e-5 & 0.7068 & -0.7068 & 0 \\ 0.0038 & 0.0004 & 9.8e-7 & 1.6e-5 & 5.7e-6 & 0.7071 & -0.7071 & -2.9e-5 \\ -0.0038 & -0.0004 & -9.8e-7 & -1.6e-5 & -5.7e-6 & -0.7071 & 0.7071 & 0 \\ 0.0053 & 0.0005 & 1.4e-6 & 2.3e-5 & 8.0e-6 & 0.9882 & 0.1528 & 0 \\ -0.0053 & -0.0005 & -1.4e-6 & -2.3e-5 & -8.0e-6 & -0.9882 & -0.1528 & 0 \\ -0.0486 & 0.9988 & 0 & -0.0003 & 0 & 0 & 0 & 0 \\ 0.0486 & -0.9988 & 0 & 0.0003 & 0 & 0 & 0 & 0 \end{bmatrix} \quad CR_1^b = \begin{bmatrix} 0.4094 \\ 10.0670 \\ 0.2045 \\ 0.6141 \\ 10.0670 \\ 0.3068 \\ 0 \\ 0.0016 \\ 1.1411 \\ 3.4232 \\ 10.0455 \\ 10.0455 \end{bmatrix}$$

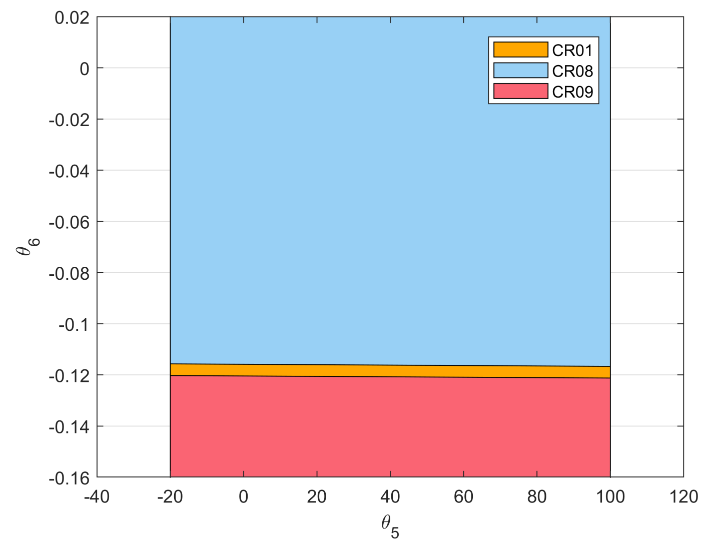


Figure B2: Partitioning of parameter space at CSTR initial states.

References

[1] P. R. Amyotte, S. Berger, D. W. Edwards, J. P. Gupta, D. C. Hendershot, F. I. Khan, M. S. Mannan, R. J. Willey, Why major accidents are still occurring, Current Opinion in Chemical Engineering 14 (2016) 1–8.

[2] R. Jarvis, A. Goddard, An analysis of common causes of major losses in the onshore oil, gas & petrochemical industries., Loss Prevention Bulletin (2017).

[3] B. Knegtering, H. Pasman, Safety of the process industries in the 21st century: A changing need of process safety management for a changing industry, Journal of Loss Prevention in the Process Industries 22 (2009) 162–168.

[4] F. Crawley, B. Tyler, HAZOP: Guide to best practice, Elsevier, 2015.

[5] Center for Chemical Process Safety, Guidelines for risk based process safety, John Wiley & Sons, 2010.

[6] J. A. G. Junior, C. M. Busso, S. C. O. Gobbo, H. Carreão, Making the links among environmental protection, process safety, and industry 4.0, Process Safety and Environmental Protection 117 (2018) 372–382.

[7] F. Khan, P. Amyotte, S. Adedigba, Process safety concerns in process system digitalization, Education for Chemical Engineers 34 (2021) 33–46.

[8] J. Lee, I. Cameron, M. Hassall, Improving process safety: What roles for digitalization and industry 4.0?, Process Safety and Environmental Protection 132 (2019) 325–339.

[9] P. G. Stoffen, Guidelines for quantitative risk assessment, Ministerie van Volkshuisvesting Ruimtelijke Ordening en Milieu. CPR E 18 (2005).

[10] H. Pasman, S. Jung, K. Prem, W. Rogers, X. Yang, Is risk analysis a useful tool for improving process safety?, Journal of Loss Prevention in the Process Industries 22 (2009) 769–777.

[11] V. Villa, N. Paltrinieri, F. Khan, V. Cozzani, Towards dynamic risk analysis: A review of the risk assessment approach and its limitations in the chemical process industry, Safety Science 89 (2016) 77–93.

[12] H. Beerens, J. Post, P. U. De Haag, The use of generic failure frequencies in qra: The quality and use of failure frequencies and how to bring them up-to-date, Journal of Hazardous Materials 130 (2006) 265–270.

[13] N. Paltrinieri, F. Khan, Dynamic risk analysis in the chemical and petroleum industry: evolution and interaction with parallel disciplines in the perspective of industrial application, Butterworth-Heinemann, 2016.

[14] A. Meel, W. D. Seider, Plant-specific dynamic failure assessment using bayesian theory, Chemical Engineering Science 61 (2006) 7036–7056.

[15] R. Kanes, M. C. R. Marengo, H. Abdel-Moati, J. Cranefield, L. Véchot, Developing a framework for dynamic risk assessment using bayesian networks and reliability data, Journal of Loss Prevention in the Process Industries 50 (2017) 142–153.

[16] R. Ferdous, F. Khan, R. Sadiq, P. Amyotte, B. Veitch, Analyzing system safety and risks under uncertainty using a bow-tie diagram: An innovative approach, Process Safety and Environmental Protection 91 (2013) 1–18.

[17] N. Khakzad, F. Khan, P. Amyotte, Dynamic risk analysis using bow-tie approach, Reliability Engineering & System Safety 104 (2012) 36–44.

[18] J. Kim, A. U. A. Shah, H. G. Kang, Dynamic risk assessment with bayesian network and clustering analysis, Reliability Engineering & System Safety 201 (2020) 106959.

[19] N. G. Leveson, G. Stephanopoulos, A system-theoretic, control-inspired view and approach to process safety, AIChE Journal (2013).

[20] F. Albalawi, H. Durand, P. D. Christofides, Process operational safety via model predictive control: Recent results and future research directions, Computers & Chemical Engineering 114 (2018) 171–190.

[21] Z. Wu, P. D. Christofides, Process Operational Safety and Cybersecurity: A Feedback Control Approach, Springer Nature, 2021.

[22] J. A. Venkidasalapathy, C. Kravaris, Safety-centered process control design based on dynamic safe set, Journal of Loss Prevention in the Process Industries 65 (2020) 104126.

[23] T. M. Ahooyi, M. Soroush, J. E. Arbogast, W. D. Seider, U. G. Oktem, Model-predictive safety system for proactive detection of operation hazards, AIChE Journal 62 (2016) 2024–2042.

[24] B. Bhadriraju, J. S.-I. Kwon, F. Khan, Risk-based fault prediction of chemical processes using operable adaptive sparse identification of systems (oasis), Computers & Chemical Engineering 152 (2021) 107378.

[25] A. Nemet, J. J. Klemeš, I. Moon, Z. Kravanja, Safety analysis embedded in heat exchanger network synthesis, Computers & Chemical Engineering 107 (2017) 357–380.

[26] A. Castillo-Landero, A. P. Ortiz-Espinoza, A. Jimenez-Gutierrez, A process intensification methodology including economic, sustainability, and safety considerations, Industrial & Engineering Chemistry Research 58 (2018) 6080–6092.

[27] Y. Tian, E. N. Pistikopoulos, Synthesis of operable process intensification systems – Steady-state design with safety and operability considerations, Industrial & Engineering Chemistry Research 58 (2018) 6049–6068.

[28] Y. Tian, M. S. Mannan, Z. Kravanja, E. N. Pistikopoulos, Towards the synthesis of modular process intensification systems with safety and operability considerations-application to heat exchanger network, in: Computer Aided Chemical Engineering, volume 43, Elsevier, 2018, pp. 705–710.

[29] E. N. Pistikopoulos, N. A. Diangelakis, R. Oberdieck, M. M. Papathanasiou, I. Nascu, M. Sun, PAROC — An integrated framework and software platform for the optimisation and advanced model-based control of process systems, Chemical Engineering Science 136 (2015) 115–138.

[30] H. Bao, F. Khan, T. Iqbal, Y. Chang, Risk-based fault diagnosis and safety management for process systems, Process Safety Progress 30 (2011) 6–17.

[31] E. N. Pistikopoulos, N. A. Diangelakis, R. Oberdieck, Multi-parametric Optimization and Control, John Wiley & Sons, 2020.

[32] V. Sakizlis, V. Dua, J. D. Perkins, E. N. Pistikopoulos, Robust model-based tracking control using parametric programming, Computers & chemical engineering 28 (2004) 195–207.

[33] M. Sun, B. Chachuat, E. N. Pistikopoulos, Design of multi-parametric nco tracking controllers for linear dynamic systems, Computers & Chemical Engineering 92 (2016) 64–77.

[34] M. T. Amin, F. Khan, Dynamic process safety assessment using adaptive bayesian network with loss function, Industrial & Engineering Chemistry Research 61 (2022) 16799–16814.

[35] C. Kravaris, I. K. Kookos, Understanding Process Dynamics and Control, Cambridge University Press, 2021.

[36] P. Rivotti, R. S. Lambert, E. N. Pistikopoulos, Combined model approximation techniques and multiparametric programming for explicit nonlinear model predictive control, Computers & Chemical Engineering 42 (2012) 277–287.

[37] J. Katz, I. Pappas, S. Avraamidou, E. N. Pistikopoulos, Integrating deep learning models and multiparametric programming, Computers & Chemical Engineering 136 (2020) 106801.

[38] N. A. Diangelakis, B. Burnak, J. Katz, E. N. Pistikopoulos, Process design and control optimization: A simultaneous approach by multi-parametric programming, AIChE Journal 63 (2017) 4827–4846.

[39] Y. Tian, I. Pappas, B. Burnak, J. Katz, E. N. Pistikopoulos, Simultaneous design & control of a reactive distillation system – A parametric optimization & control approach, Chemical Engineering Science 230 (2021) 116232.

[40] R. Oberdieck, E. N. Pistikopoulos, Explicit hybrid model-predictive control: The exact solution, Automatica 58 (2015) 152–159.

[41] Chemical Safety Board, T2 laboratories inc. reactive chemical explosion, https://www.csb.gov/t2-laboratories-inc-reactive-chemical-explosion/ (2009).

[42] T. Stauffer, Making the most of alarms as a layer of protection, in: Safety Control Systems Conference-IDC Technologies, 2010.

[43] EEMUA Publication 191, Alarm systems: A guide to design, management, and procurement (2007).

[44] O. Palma-Flores, L. A. Ricardez-Sandoval, Simultaneous design and nonlinear model predictive control under uncertainty: A back-off approach, Journal of Process Control 110 (2022) 45–58.

[45] M. Rafiei, L. A. Ricardez-Sandoval, A trust-region framework for integration of design and control, AIChE Journal 66 (2020) e16922.

[46] L. Narraway, J. Perkins, Selection of process control structure based on economics, Computers & chemical engineering 18 (1994) S511–S515.

[47] R. Oberdieck, N. A. Diangelakis, M. M. Papathanasiou, I. Nascu, E. N. Pistikopoulos, POP – Parametric optimization toolbox, Industrial & Engineering Chemistry Research 55 (2016) 8979–8991.

[48] K. I. Kouramas, C. Panos, N. P. Faísca, E. N. Pistikopoulos, An algorithm for robust explicit/multi-parametric model predictive control, Automatica 49 (2013) 381–389.

[49] E. Zhang, P. Feissel, J. Antoni, A comprehensive bayesian approach for model updating and quantification of modeling errors, Probabilistic engineering mechanics 26 (2011) 550–560.

[50] Y. Zheng, Z. Wu, Physics-informed online machine learning and predictive control of nonlinear processes with parameter uncertainty, Industrial & Engineering Chemistry Research 62 (2023) 2804–2818.

[51] A. Braniff, M. A. A. Masud, Y. Tian, Fault-prognostic model predictive control with physics-data driven monitoring, American Control Conference (2023).

[52] L. Hewing, K. P. Wabersich, M. Menner, M. N. Zeilinger, Learning-based model predictive control: Toward safe learning in control, Annual Review of Control, Robotics, and Autonomous Systems 3 (2020) 269–296.

[53] S. Gros, M. Zanon, R. Quirynen, A. Bemporad, M. Diehl, From linear to nonlinear mpc: bridging the gap via the real-time iteration, International Journal of Control 93 (2020) 62–80.

[54] D. A. Allan, C. N. Bates, M. J. Risbeck, J. B. Rawlings, On the inherent robustness of optimal and suboptimal nonlinear mpc, Systems & Control Letters 106 (2017) 68–78.

[55] L. T. Biegler, A perspective on nonlinear model predictive control, Korean Journal of Chemical Engineering 38 (2021) 1317–1332.

[56] Y. Cao, J. Kang, Z. K. Nagy, C. D. Laird, Parallel solution of robust nonlinear model predictive control problems in batch crystallization, Processes 4 (2016) 20.

[57] T. Faulwasser, L. Grüne, M. A. Müller, et al., Economic nonlinear model predictive control, Foundations and Trends® in Systems and Control 5 (2018) 1–98.

[58] I. J. Wolf, W. Marquardt, Fast nmpc schemes for regulatory and economic nmpc–a review, Journal of Process Control 44 (2016) 162–183.

[59] L. Biegler, X. Yang, G. Fischer, Advances in sensitivity-based nonlinear model predictive control and dynamic real-time optimization, Journal of Process Control 30 (2015) 104–116.

[60] Z. Zhang, Z. Wu, D. Rincon, P. D. Christofides, Real-time optimization and control of nonlinear processes using machine learning, Mathematics 7 (2019) 890.

[61] I. Pappas, N. A. Diangelakis, E. N. Pistikopoulos, Multiparametric/explicit nonlinear model predictive control for quadratically constrained problems, Journal of Process Control 103 (2021) 55–66.