Dynamic Risk-based Design and Explicit Model Predictive Control via Multi-Parametric Programming

Moustafa Ali [a], Xiaoqing Cai [a], Faisal Khan [b], Yuhe Tian [c] [1]

[a] Texas A&M Energy Institute, Texas A&M University, College Station, TX

[b] Mary Kay O'Connor Process Safety Center, Artie McFerrin Department of Chemical Engineering, Texas A&M University, College Station, TX

[c] Department of Chemical and Biomedical Engineering, West Virginia University, Morgantown, WV

Abstract

We have introduced an integrated approach to synergize design optimization, explicit model predictive control (MPC), and dynamic risk assessment for real-time process safety management. It follows a step-wise procedure which features: (i) High fidelity modeling of the process and safety system, (ii) Dynamic risk modeling as a function of process variable(s), (iii) Computation of design-dependent, risk-aware control policies via multi-parametric programming, and (iv) Dynamic optimization to close the loop with optimal design, operating, and risk control decisions. Multi-faceted process systems and safety factors can thus be systematically addressed via the resulting single mixed-integer dynamic programming problem: (a) Explicit incorporation of safety-critical variable bounds as path constraints in MPC formulation, (b) Optimal control of risk accounting for the impact of multi-variate interactions and uncertainties on fault probability and severity, and (c) Control-aware fault prognosis and proactive risk mitigation to moderate fault severity and raise alarm ahead of a sufficiently long time when necessary. A real-world case study on a continuous stirred tank reactor at the T2 Laboratories will be presented to demonstrate the proposed strategy.

Keywords

Model predictive control, Dynamic risk assessment, Fault prognosis, Multi-parametric programming, Design and control.

1. Introduction

Process safety management (PSM) is unequivocally a key priority for chemical and energy manufacturing industries. Accidents in chemical plants to date have caused severe human and cost losses with pressing societal and environmental issues (Jarvis and Goddard, 2017; Amyotte et al., 2016). The ongoing trend towards digital supply networks and real-time decision making also poses new challenges to PSM with more complex, dynamic, integrative, and automated process plants (Junior et al., 2018). Thus, there is an imperative need to bridge the link between safety-critical decision making with systems-based real-time operation to maximally reduce process safety losses in a dynamic manner, as a step change from the current practices relying on passive protection layers (Lee et al., 2019; Leveson and Stephanopoulos, 2013).

Quantitative risk assessment has been the subject of extensive research which adapts analytic methodologies to estimate the probability of failure occurrence and severity of consequences, however at a given time of the process facility life cycle (Witter, 1992). Burgeoning research efforts have been made on dynamic risk assessment to achieve timely-updated and process-specific risk estimation using Bayesian Network approaches integrated with bow-tie diagram, event tree analysis, etc. (Meel and Seider, 2008; Villa et al., 2016; Kanes et al., 2017) Dynamic safety management has also been addressed from a control-oriented perspective as to maintaining safety-critical process variables (e.g., temperature, pressure) within the pre-specified safe operating region (or bounds). Model predictive control (MPC) is typically leveraged due to the ability to explicitly consider path constraints and forecast future trajectory via the moving horizon policy (Ahooyi et al., 2016; Bhadriraju et al., 2021). Theoretical approaches have also been proposed to reversely identify a maximal set of process states within which safe and stable operation is guaranteed despite disturbances (Albalawi et al., 2018; Venkidasalapathy and Kravaris, 2020). However, there exists a missing link to quantify the impact of physics-based multivariate interactions and dynamic variations on process

[1] Corresponding author. Email: yuhe.tian@mail.wvu.edu

risk. A holistic risk-based control optimization approach is also lacking which can integrate the multiple decision making time scales of design, control, and risk to identify the economically optimal design and operational solutions with proactive process safety management.

To address these challenges, in this work, we present a systematic approach for dynamic risk-based process design and control optimization on the basis of the PAROC (PARametric Optimization and Control) framework (Pistikopoulos et al., 2015). The rest of the paper is organized as follows: Section 2 states the proposed framework for simultaneous design and control with dynamic risk considerations, Section 3 showcases the methodology step-by-step on an exothermic continuous stirred tank reactor at the T2 Laboratories.

2. The Framework for Dynamic Risk-based Design and Control Optimization

The proposed framework is presented in Fig. 1 for the integration of dynamic risk assessment with design and control decision making, thus optimizing the operational trajectory with the ability of proactive risk management and fault prognosis through multiple time scales. The step-wise procedure is detailed in what follows.

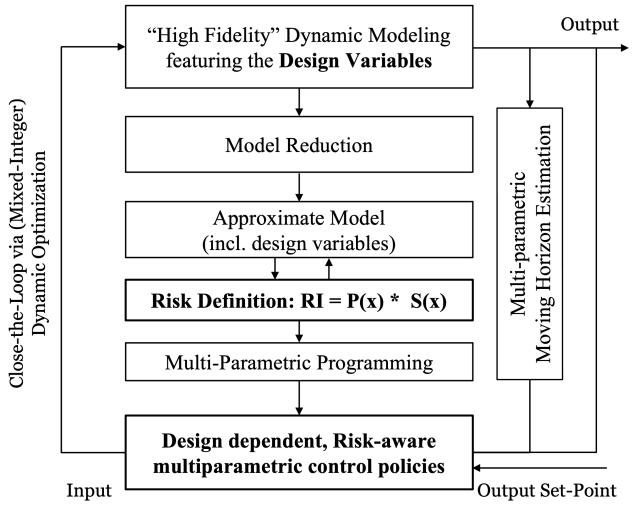

Figure 1: The proposed framework.

Step 1: High fidelity dynamic modeling

This steps aims to develop a first principles dynamic model which can rigorously describe the typically highly nonlinear process system dynamics using a system of (Partial) Differential-Algebraic Equations (Eq. 1). Design variables, in the form of continuous or binary variables, can be formulated as degrees of freedom to be optimally determined through the framework. To the interest of this work, the dynamics for the safety system can also be accounted for with continuous and discrete decision variables (e.g., operating mode switch, open or close of pressure relief valve).

$$\begin{aligned} \frac{d}{dt}x(t) &= f(x(t),u(t),Y(t),d(t),De) \\ y &= g(x(t),u(t),Y(t),d(t),De) \end{aligned} \tag{1}$$

where x is the vector of states, u defines input variables, y represents output variables, Y gives binary variables, d denotes disturbances, and De defines design variables.

Step 2: Model approximation

As shown in Eq. 2, a linear state space model is derived from the above high fidelity model via model reduction, systems identification, or data-driven approaches (Rivotti et al., 2012; Katz et al., 2020). The approximated model preserves sufficient modeling accuracy with reduced numerical complexity, thus enabling the implementation of optimal control strategies in the next steps.

$$\begin{aligned} x_{k+1} &= Ax_k + Bu_k + C[d_k; De] \\ y_k &= Dx_k \end{aligned} \tag{2}$$

where A,B,C,D are constant matrices, subscript k denotes the current time step, x is the vector of identified states, which can have physical meanings or not based on the selected model reduction techniques, De is explicitly retained for design-dependent controller design.

Step 3: Dynamic risk modeling

In this work, we adapt the dynamic risk model proposed by Bao et al. (2011), in which risk is defined as a function of time-dependent safety-critical process variable(s) allowing for real-time safety monitoring and model-based forecasting. Prior to the risk assessment, abnormality identification is first conducted to survey historical cases and perform open loop/near miss simulations to the specific process system to locate any potential faults and the corresponding safety-critical process variables (which can be directly measurable or implicitly inferential). Herein, the occurrence of a fault is defined by the risk exceeding a certain threshold value, whereas risk (RI) is calculated via Eq. 3:

$$RI = P(x) \times S(x) \tag{3}$$

- **Fault probability $\mathbf{P(x)}$** – which is determined as the statistical probability of the safety-critical variable(s) $x(t)$ to exceed the upper/lower control limit (UCL, LCL) using normal distribution. The UCL and LCL are respectively defined as 3 standard deviations (σ) away from the nominal operating point (μ), since statistically 99.7% of the values lie in the region of $\mu \pm 3\sigma$ (i.e., the three-sigma rule). Thus, the fault probability is calculated as below (taking the example of $x > \mu$):

$$P(x) = \phi[\frac{x-(\mu+3\sigma)}{\sigma}] \tag{4}$$

- **Fault severity $\mathbf{S(x)}$** – which quantifies the severity of potential hazard as an exponential function of the deviation of the safety-critical variable(s) (when $x > \mu$):

$$S(x) = 100^{\frac{x-(\mu+3\sigma)}{x-\mu}} \tag{5}$$

The following advantageous features are offered by the above quantitative risk model: (i) Instantaneous updates of the fault probability and severity as a function of the *deviation* of safe-critical variable(s); (ii) At $\mu \pm 3\sigma$, $P(x)$ is mathematically *standardized* at 0.5 and $S(x)$ at 1 which provide a consistent benchmark between different processes, design, or operating conditions; (iii) Risk RI follows a *pseudo-exponential* growth function with increasingly faster propagation as approaching the risk threshold (as illustrated in Fig. 2).

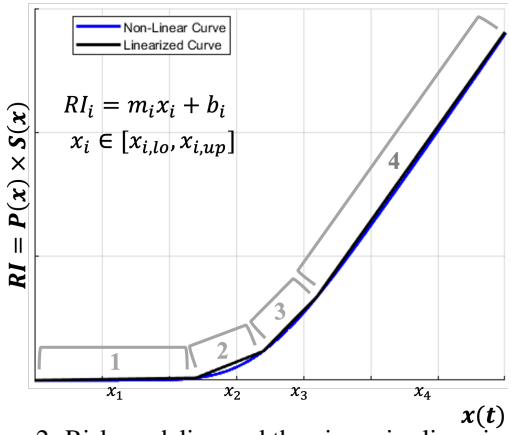

Figure 2: Risk modeling and the piecewise linearization.

The resulting dynamic risk model is linearized using piecewise affine functions which enable to design linear MPC. More importantly, the *RI* piecewise linearization characterizes different regions of risk with distinct propagation speeds, based on which the risk control objective can be automatedly adjusted. For example, to sustain stable operation when *RI* lies in region 1, to prioritize risk control in region 2, or to adapt aggressive risk control in regions 3 and 4.

Step 4: Integrated process and risk modeling

An integrated linear state space model is formulated which describes the process system dynamics and the risk dynamics (Eqs. 6b-c). Mixed-integer variables (Eqs. 6d-e) are introduced to provide a unified mathematical expression for the piecewise risk model.

Step 5: Design-dependent risk-based multi-parametric MPC

The design-dependent risk-based model predictive control problem is presented in Eq. 6, which offers **dual layers of proactive process safety management**: (i) Model-based risk assessment as an overarching metric, (ii) Bounded safe region for states via MPC path constraints. Though approximated linear model is used for controller design, closed-loop validation is performed in Step 6 which tests the controller on the original nonlinear process and risk model to ensure the actual risk control performance.

$$min_u \; J = x_N^T P x_N + \sum_{k=1}^{OH-1} \left((y_k - y_k^R)^T Q R_k \left(y_k - y_k^R\right)\right) + \sum_{k=0}^{CH-1} \left(\Delta u_k - \Delta u_k^R\right)^T R1_k \left(\Delta u_k - \Delta u_k^R\right) \tag{6a}$$

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

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

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

$$\sum_i y_i = 1 \qquad y_i \in \{0,1\} \qquad x_{i,lo} y_i \le x_i \le x_{i,up} y_i \tag{6e}$$

$$\overline{x} \le x \le \underline{x} \qquad \overline{u} \le u \le \underline{u} \tag{6f}$$

$$\overline{y} \le y \le \underline{y} \qquad \overline{RI} \le RI \le \underline{RI} \tag{6g}$$

where y_i is binary variable for *RI* discretization, P is terminal weight, QR and R are controller weights, CH and OH are control and output horizons, superscript R is setpoint, other nomenclature follow the previous steps.

The MPC problem will be reformulated and solved via multi-parametric mixed-integer quadratic programming (mp-MIQP). Multi-parametric model predictive control (mp-MPC) generates explicit control law, expressed as affine functions of the defined parametric set (e.g., disturbance, state variables, design variables, and extended to include risk in this study). In this way, MPC online optimization can be replaced with mp-MPC optimal look-up maps which are generated *in priori* via offline optimization, leading to improved online computational efficiency (Pistikopoulos et al., 2020).

Step 6: Fault-prognostic design and control optimization

A single mixed-integer dynamic optimization problem is formulated at this step to identify the optimal design and control decisions with dynamic risk considerations (as shown in Eq. 7). The key features include: (i) an objective function with process safety, product quality, and/or economic considerations (Eq. 7a), (ii) closed-loop optimization based on the high-fidelity form of the process and risk model (Eqs. 3b-d), (iii) multi-parametric risk-based controller designed as per Step 5 (Eqs. 7e-f), (iv) bounds for risk and safety-critical variables explicitly considered (Eqs. 7g-i), and (v) design variables to be optimized while directly accounting for their impacts on control and dynamic risk (i.e., u_T as a function of *De*). Additionally, the dynamic optimizer introduces a middle-term decision making layer empowering the flexible selection for the fault prognosis horizon (τ), which is fully connected but independent with the short-term control and long-term design decisions. This would open up the application of this methodology in many fast, slow, or hybrid process systems.

$$min \; F = \int_0^{\tau} P(x,y,u,Y,d,De,RI)dt \tag{7a}$$

$$\text{s.t.} \quad dx/dt = f(x,y,u,Y,d,De) \tag{7b}$$

$$y = g(x,u,Y,d,De) \tag{7c}$$

$$RI = s(x,u,Y,d,De) \tag{7d}$$

$$u_T = K_i \theta_T + r_i \qquad \theta_T \in CR^i = \{CR_i^A \theta \le CR_i^b\} \tag{7e}$$

$$\theta_T = [x_T, y_T, y_T^R, Y, d_T, De, RI] \tag{7f}$$

$$\underline{x} \le x \le \overline{x} \qquad \underline{u} \le u \le \overline{u} \tag{7g}$$

$$\underline{y} \le y \le \overline{y} \qquad \underline{De} \le De \le \overline{De} \tag{7h}$$

$$\overline{RI} \le RI \le \underline{RI} \qquad Y \in \{0,1\}^q \tag{7i}$$

3. Case Study: Exothermic CSTR at T2 Laboratory

3.1. Process description

In December 2007, an accident occurred at the T2 Laboratory in Florida, USA, which unfortunately killed 4 people and injured 28 others (Chemical Safety Board, 2009). Due to the inadequate cooling system, runaway reaction took place at the involved exothermic reactor which eventually led to the explosion of hydrogen and other flammable products. In this work, we will apply the proposed framework for safety-critical control and fault prognosis of this process. A continuous stirred tank reactor (CSTR) will be studied at similar conditions to the original batch reactor at T2 Laboratories.

The T2 process is conceptualized as shown in Fig. 3. The CSTR has two feed streams, comprising A (methylcyclopentadiene) in solution S (diglyme) and B (molten sodium). To

initiate the reactions, the feeds should be preheated to a given temperature before entering the CSTR. The reaction schemes and kinetic parameters are adapted from Venkidasalapathy and Kravaris (2020). Reactor temperature T is the safety-critical variable, which should be regulated at a setpoint (e.g., 460 K) despite possible fluctuations in the feed temperature T_0. Cooling is performed through an evaporating water jacket, where the heat transfer coefficient U can be manipulated by adjusting the cooling water flow rate. The high risk region is defined according to $T \geq 480K$, entering which uncontrollable reactor temperature surge is at higher probability to occur due to the rapidly increasing side reaction rates. The **real-time PSM objectives for this case study** are to:

- Control the risk at a desired level with optimal design and operating decisions under disturbances,
- If reactor runaway cannot be avoided, attenuate the risk propagation speed and consequence severity while raising the alarm 10 minutes ahead of fault occurrence time for operator response.

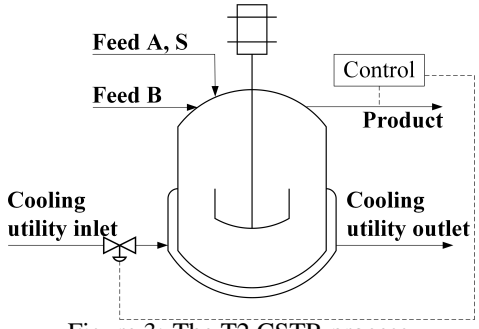

Figure 3: The T2 CSTR process.

3.2. Dynamic risk-based design and control optimization

In what follows, we present the step-by-step application of the proposed framework to this T2 CSTR process.

3.2.1. CSTR dynamic modeling and model approximation

We assume the use of an ideal CSTR with constant reactor volume. Dynamic mass and energy balances are utilized to construct the high fidelity model for this T2 CSTR process as listed in Eq. 8. The major process variables and parameters are summarized in Table 1.

$$\frac{dC_A}{dt} = \frac{F_{A,in}}{V} - \frac{q_{out}}{V}C_A - k_1(T)C_AC_B \tag{8a}$$

$$\frac{dC_B}{dt} = \frac{F_{B,in}}{V} - \frac{q_{out}}{V}C_B - k_1(T)C_AC_B \tag{8b}$$

$$\frac{dC_S}{dt} = \frac{F_{S,in}}{V} - \frac{q_{out}}{V}C_S - k_2(T)C_S \tag{8c}$$

$$\frac{dT}{dt} = \frac{q_{out}}{V}(T_{in} - T) + \frac{\sum(-\Delta H_k)r_k}{\rho c_p} - \frac{UA_x(T - T_c)}{\rho c_p V} \tag{8d}$$

Table 1: List of major process variables.

State variables	C_A, C_B, C_S: Concentrations, T: Temperature
Input variable	U: Heat transfer coefficient
Disturbance	T_0: Feed temperature
Design variable	U_{max}: Maximum heat transfer coefficient
Parameters	F_{A0}, F_{S0}, F_{B0}: Feed flowrates (1050, 525, 1250 mol/h) V: Volume (4000 L), ρ: Mixture density (36 mol/L) c_p: Specific heat (430.91 J/mol·K) A_x: Heat transfer area (5.3 m^2), T_c: Coolant (373 K)

The resulting dynamic model is linearized around its steady state to obtain an approximated state space model as shown in Eq. 9. Note that in this case study, the design variable U_{max} is addressed in the MPC path constraints instead of explicitly appearing in the state equations. A control time step of 1 minute is selected.

$$\begin{bmatrix} \overline{C_A} \\ \overline{C_B} \\ \overline{C_S} \\ \overline{T} \end{bmatrix}_{k+1} = A \begin{bmatrix} \overline{C_A} \\ \overline{C_B} \\ \overline{C_S} \\ \overline{T} \end{bmatrix}_k + B\overline{U}_k + C\overline{T}_{in,k} \tag{9}$$

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

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

where the deviation variables are defined as $\overline{X} = X - X_{ss}$.

3.2.2. Dynamic risk modeling and piecewise linearization

Next, to model the dynamic risk as a function of reactor temperature (i.e. the safety-critical variable), we adapt μ as the normal reactor operating temperature at 460 K and σ as a deviation of 5 K to define UCL at 475 K. *RI* can thus be quantified as per Eqs. 3-5, with the high risk region defined as $RI \geq 2.82$ in accordance with $T \geq 480K$. The pseudo-exponential function of *RI* is approximated using piecewise linearizations. Four affine functions are identified to describe the risk propagation trajectory ranging from the normal operating point to the high risk region (Fig. 2). In sum, Eq. 10 shows the output equation of deviation variable $\overline{RI}$ ($\overline{RI} = RI - b$) against the CSTR state variable $\overline{T}$. Note that k is a variable determined from Eq. 11, instead of a parameter with a constant value.

$$\overline{RI}_k = \begin{bmatrix} 0,0,0,k \end{bmatrix} \begin{bmatrix} \overline{C_A} \\ \overline{C_B} \\ \overline{C_S} \\ \overline{T} \end{bmatrix}_k \tag{10}$$

$$k = \begin{cases} 0.0078, & T \in [460, 472] \\ 0.2147, & T \in [472, 477] \\ 0.5496, & T \in [477, 481] \\ 0.7629, & T \in [481, 495] \end{cases} \tag{11}$$

3.2.3. Risk-based multi-parametric controller design

Built on the integrated process and risk model comprising Eqs. 9-10, a mp-MPC problem is formulated to achieve optimal dynamic risk management. The controller tuning parameters are presented in Table 2. Since the T2 CSTR dynamics is relatively slow with the controller time step as 1 min, we first select $OH = 10$ which enables a 10-min fault-prognostic period just relying on MPC moving horizon estimation. In a later step, we will showcase the decoupling of controller output horizon with the desired fault prognosis period.

Table 2: mp-MPC tuning parameters.

OH	CH	QR	$R1$
10	1	10^4	10^{-6}

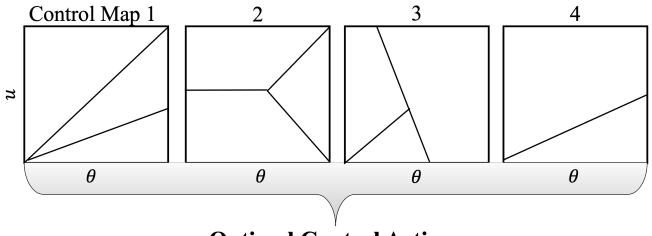

Figure 4: mp-MIQP solution as a superset of mp-QPs.

The mp-MPC problem is further converted to a mp-MIQP problem, in which the binary variables are introduced by *RI* piecewise linearization. Due to the small combinatorial space with the involved binary variables being mutually exclusive, we solve the mp-MIQP by enumerating all the four possible integer solutions and generating a superset of mp-QP solution maps as depicted in Fig. 4. The actual solution of mp-MIQP is therefore determined by mapping through the mp-QP maps on their respective valid piecewise regions. Using the tuning parameters in Table 2, each mp-QP problem is solved to have 59 critical regions with 8 parameters (i.e., 4 state variables, *RI* as output variable, *RI* setpoint, disturbance, and design variable U_{max} as in path constraint $U_{min} \leq U \leq U_{max}$). This approach can be readily applied to large-scale process systems with extended combinatorial space by using decomposition-based mp-MIQP algorithms (Oberdieck and Pistikopoulos, 2015).

To verify the controller performance, we perform closed-loop validation against the original nonlinear CSTR and risk model. The CSTR initial state is at 460 K and a step change of the disturbance is introduced at $t = 0$ with $\Delta T_{in} = 25K$. As shown in Fig. 5, without controller on, the open-loop process will reach the high risk region after around 9 hours followed by risk surge. However, with the derived risk-based multi-parametric controller, the risk can be well controlled at a low level of $RI \approx 0$ for the entire operating time. The controller is also tested to stabilize reactor operation at a medium risk level, which may offer a higher productivity with higher reactor temperature. In this regard, we select the dynamic risk setpoint at 0.74 which lies between the upper control limit and the high risk limit. As presented in Fig. 6, the risk-based mp-MPC is able to effectively track the desired dynamic risk setpoint as well as control it from escalation.

Under certain conditions, the process risk cannot be saved from eventually evolving into the high risk region. An indicative scenario is illustrated in Fig. 7 due to notably larger disturbances, less coolant availability (U_{max}), and/or more stringent high risk limit. In this case, an alarm is raised at $t = 11.13\,h$ when mp-MPC predicts the risk to enter high risk region over the next 10-min output horizon, and the risk actually reaches the limit at $t = 11.35\,h$. A fault prognosis horizon of 13.2 min is thus enabled which allows the operators to plan for abnormality response prudently. It is also worth pointing out that, while waiting for operator intervention, the risk-based mp-MPC continues working to substantially mitigate the risk propagation speed and consequence severity compared to open-loop operation.

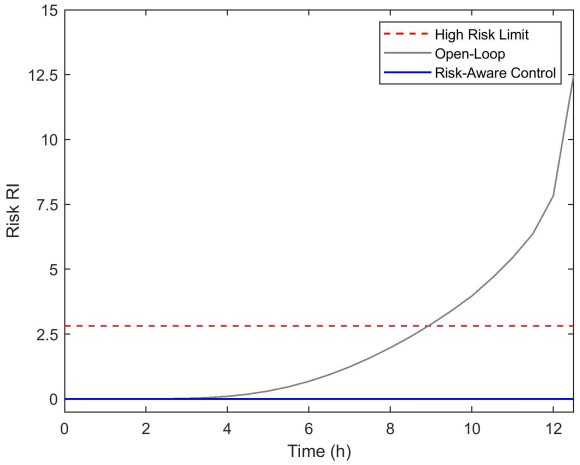

Figure 5: Closed-loop control at low level of risk.

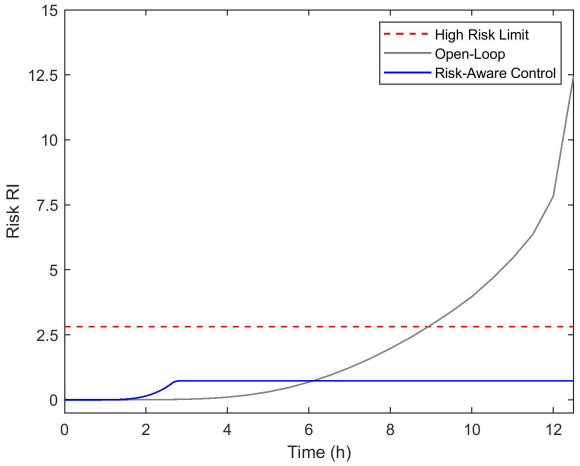

Figure 6: Closed-loop control at medium level of risk.

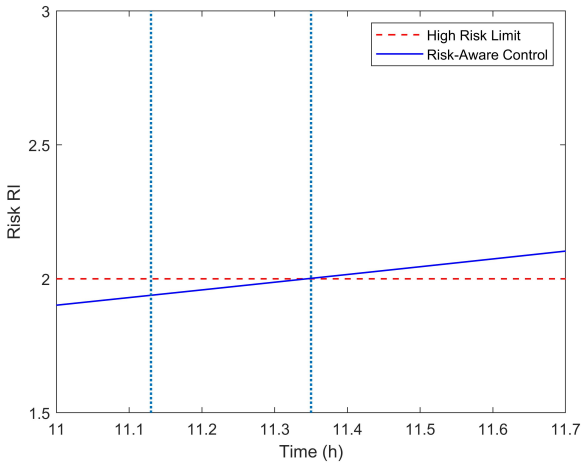

Figure 7: Fault prognosis and alarm raising leveraging MPC moving horizon estimation.
$t = 11.13\,h$: alarm is raised for predicted high risk operation
$t = 11.35\,h$: dynamic risk reaches high risk region

3.2.4. Integrated design and control with fault prognosis

We further investigate fault-prognostic design and operational optimization following Eq. 7. The objective function is set as Eq. 12. τ is the fault prognosis time horizon via the online dynamic optimizer, which decouples the pro-

cess safety forecasting from mp-MPC moving horizon estimation. A fault prognosis horizon of 10 minutes is selected in consistence with section 3.2.3, while can be flexibly shortened or prolonged based on need. Moreover, we can reduce the multi-parametric control output horizon (OH) from 10 to 2 which helps to relax the controller decision making complexity. Under the scenario of low level risk control optimization ($RI \leq 0.002$), the optimal design is identified as $U_{max} = 48.2\ kJ/(K \cdot h \cdot m^2)$ versus the original value of $U_{max} = 55.0\ kJ/(K \cdot h \cdot m^2)$ adapted from open literature. The average operating cost is $U_{max} = 41.5\ kJ/(K \cdot h \cdot m^2)$.

$$min\ \ F = \sum_{0}^{\tau} U/\tau + WU_{max} \tag{12}$$

where $\sum_0^\tau U/\tau$ accounts for the operating cost with U as a near-linear function of utility cooling water flowrate, WU_{max} is an indicator for design cost with W as a weight factor.

Conclusion

We have introduced an integrated design and multi-parametric model predictive control framework for operational optimization and dynamic risk-based process safety management. Ongoing work focuses on the extension to an error-tolerant risk-based control and optimization approach accounting for model approximation mismatch in process safety-critical system applications.

References

Ahooyi, T. M., M. Soroush, J. E. Arbogast, W. D. Seider, and U. G. Oktem (2016). Model-predictive safety system for proactive detection of operation hazards. *AIChE Journal 62*(6), 2024–2042.

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

Amyotte, P. R., S. Berger, D. W. Edwards, J. P. Gupta, D. C. Hendershot, F. I. Khan, M. S. Mannan, and R. J. Willey (2016). Why major accidents are still occurring. *Current opinion in chemical engineering 14*, 1–8.

Bao, H., F. Khan, T. Iqbal, and Y. Chang (2011). Risk-based fault diagnosis and safety management for process systems. *Process Safety Progress 30*(1), 6–17.

Bhadriraju, B., J. S.-I. Kwon, and F. Khan (2021). Oasis-p: Operable adaptive sparse identification of systems for fault prognosis of chemical processes. *Journal of Process Control 107*, 114–126.

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

Jarvis, R. and A. Goddard (2017). An analysis of common causes of major losses in the onshore oil, gas & petrochemical industries. *Loss Prevention Bulletin* (255).

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

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

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

Lee, J., I. Cameron, and M. Hassall (2019). Improving process safety: What roles for digitalization and industry 4.0? *Process safety and environmental protection 132*, 325–339.

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

Meel, A. and W. D. Seider (2008). Real-time risk analysis of safety systems. *Computers & Chemical Engineering 32*(4-5), 827–840.

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

Pistikopoulos, E. N., N. A. Diangelakis, and R. Oberdieck (2020). *Multi-parametric Optimization and Control*. John Wiley & Sons.

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

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

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

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

Witter, R. E. (1992). Guidelines for hazard evaluation procedures. *Plant/Operations Progress;(United States) 11*(2).