Systems & Control Transactions

Research Article - Peer Reviewed Conference Proceeding
ESCAPE 35 - European Symposium on Computer Aided Process Engineering
Ghent, Belgium. 6-9 July 2025
Jan F.M. Van Impe, Grégoire Léonard, Satyajeet S. Bhonsale,
Monika E. Polańska, Filip Logist (Eds.)

PSE PRESS

Integrating Dynamic Risk Assessment with Explicit Model Predictive Control via Chance-Constrained Programming

Sahithi Srijana Akundi[a,b,c], Yuanxing Liu[a,b,c], Austin Braniff[d], Beatriz Dantas[d], Shayan S Niknezhad[a], Faisal Khan[b,c], Yuhe Tian[d], Efstratios N Pistikopoulos[a,c]*

[a] Texas A&M Energy Institute, Texas A&M University, College Station, TX, USA
[b] Mary Kay O'Connor Process Safety Center (MKOPSC), Texas A&M University, College Station, TX, USA
[c] Artie McFerrin Department of Chemical Engineering, Texas A&M University, College Station, TX, USA
[d] Department of Chemical and Biomedical Engineering, West Virginia University, Morgantown, WV, USA
* Corresponding Author: stratos@tamu.edu.

ABSTRACT

Maintaining operational efficiency while ensuring safety is a longstanding challenge in industrial process control, particularly in high-risk environments. This paper presents a novel Dynamic Risk-Informed Explicit Model Predictive Control (R-eMPC) framework that integrates safety and operational objectives using probabilistic constraints and real-time risk assessments. Unlike traditional approaches, this framework dynamically adjusts safety thresholds based on Bayesian updates, ensuring a balanced trade-off between reliability and efficiency. The validation of this approach is illustrated through a case study on tank level control, a safety-critical process where maintaining the liquid level within predefined safety limits is paramount. The results demonstrate the framework's capability to optimize performance while maintaining robust safety margins. By emphasizing adaptability and computational efficiency, this research provides a scalable solution for integrating safety into real-time control strategies for similar process systems.

Keywords: Model predictive control, Bayesian risk analysis, Dynamic risk assessment, Safety-aware control, Multi-parametric programming, Chance-constrained programming

INTRODUCTION

Industrial operations, particularly in chemical plants, carry an inherent risk of catastrophic incidents, posing threats to both human safety and the environment [1]. These risks have driven extensive research and the development of systematic methods to enhance process functional safety [2]. While traditional safety measures, such as Hazards and Operability analysis and fault tree analysis [3], have significantly contributed to accident prevention, the increasing complexity of industrial processes necessitates advanced optimization, control, and machine learning techniques capable of integrating safety and performance objectives seamlessly [4,5].

Traditional Model Predictive Control (MPC) frameworks, though widely adopted, rely on rigid constraints to enforce safety, often leading to overly conservative operations [6]. Recent efforts have explored merging safety principles with MPC through adaptive, learning-based [7], and probabilistic approaches [8,9]. However, these methods often fall short in dynamically quantifying and updating risk parameters in real time, limiting their applicability in highly dynamic and uncertain environments [10].

This paper addresses these gaps by introducing the Dynamic Risk-Informed Model Predictive Control (R-eMPC) framework. Inspired by dynamic risk-based design and optimization principles [11], R-eMPC incorporates Bayesian updates and chance-constrained programming to dynamically adjust safety thresholds along a receding horizon [12]. This integration ensures a robust balance between safety and operational efficiency while responding to real-time process variations. The proposed framework is systematically applied to a tank-level control case study, demonstrating its potential for scalable and adaptive safety-critical applications.

The remainder of this paper is organized as follows: Section 2 introduces the case study, providing the context and system dynamics for evaluating the proposed framework. Section 3 details the R-eMPC methodology

and demonstrates its sole application to the case study of tank level control. Section 4 present results and discusses the implications of the framework, while Section 5 concludes with key findings and outlines potential future research directions.

TANK-LEVEL CONTROL CASE STUDY

The tank level control system serves as a representative case study to evaluate the proposed R-eMPC framework (Figure 1). In industrial operations, precise regulation of the liquid level within a storage tank is crucial to prevent safety-critical incidents. Overflow scenarios may result in hazardous spills with severe environmental and operational consequences, while underflow conditions can disrupt downstream processes, leading to inefficiencies and potential system failures. The inherent dynamics and uncertainty associated with this system make it an ideal testbed for assessing the efficacy of the proposed methodology.

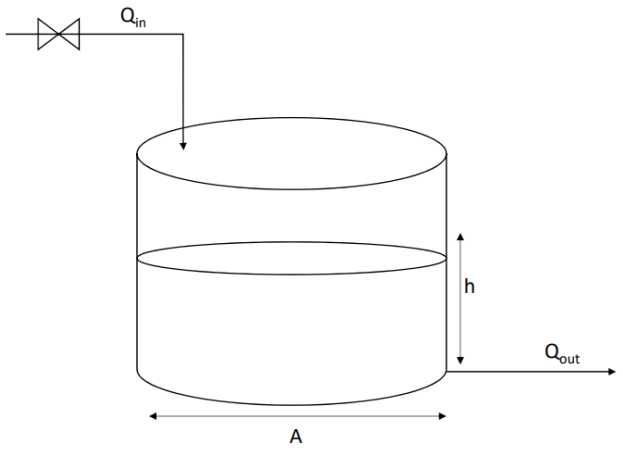

Figure 1. The schematic of the tank-filling system

The control system is designed to manage the liquid level by regulating the inflow, while the outflow is governed by the tank's current level and outlet characteristics. The system dynamics are mathematically described as:

$$\frac{dh(t)}{dt} = \frac{Q_{in}(t) - Q_{out}(t)}{A} + \frac{w(t)}{A} \quad (1)$$

where
$h(t)$ represents the liquid level
$Q_{in}(t)$ represents the inflow
$Q_{out}(t)$ represents the outflow
A represents the cross-sectional area of the tank

$w(t)$ captures external disturbances that influence the system. The primary control objective is to maintain $h(t)$ within predefined safety limits while optimizing operational performance, even in the presence of uncertainties and dynamic variations.

The choice of the tank level control system as a case study is motivated by its direct relevance to the challenges of managing safety-critical processes under dynamic and uncertain conditions. This system exemplifies the interplay between operational constraints and safety requirements, where deviations in liquid levels can result in hazardous overflows or disruptive underflows. Traditional control strategies, which often rely on static constraints, struggle to accommodate real-time disturbances, leading to conservative or infeasible operations. By applying the R-eMPC framework, this study aims to bridge this gap by integrating dynamic risk assessment and probabilistic constraints into the control process. The framework's ability to adaptively balance safety and efficiency under varying conditions underscores its potential for broader applications in safety-critical process control.

RISK- INFORMED EXPLICIT MPC FRAMEWORK

In this section, we introduce a stochastic control framework as an extension to 'Dynamic Risk-based Design and Control Optimization framework' developed in [11]. This framework serves as a comprehensive approach for the seamless integration of safety and control elements, achieved through the dynamic inclusion of risk factors within a controller optimization framework. This unique approach facilitates real-time monitoring of risk levels and the implementation of adaptive control strategies. The ensuing section provides a step-by-step elucidation of the procedural aspects of this framework.

The R-eMPC framework under discussion represents a nuanced and adaptive approach to address the complexities inherent in managing uncertain systems. This innovative paradigm seamlessly blends several pivotal elements. Firstly, it employs a Receding Horizon MPC strategy, continuously optimizing control inputs while considering the dynamics of the evolving system. Secondly, it introduces a dynamic probabilistic constraint, strategically integrating real-time risk management into the control framework to maintain system operation within predefined risk thresholds. Complementing this, a Bayesian update mechanism is seamlessly incorporated, allowing for the dynamic adaptation of these risk thresholds based on live system observations. This integrated approach represents a comprehensive strategy that not only prioritizes safety but also enables the system to adaptively optimize its performance within the realm of uncertainties—a pragmatic and adaptable solution for contemporary engineering challenges. The implementation of the framework is given below:
R-eMPC:

$$min_u\ J = x_N^T P x_N + \sum_{k=1}^{OH-1} \left(\left(y_k - y_k^R\right)^T Q R_k \left(y_k - y_k^R\right) \right) \quad (2a)$$

$$+ \sum_{k=0}^{CH-1} \left(\Delta u_k - \Delta u_k^R\right)^T R_k \left(\Delta u_k - \Delta u_k^R\right) + f(x_k)$$

s.t. $$x_{k+1} = Ax_k + Bu_k + C[d_k, De] \quad (2b)$$

$$y_k = Dx_k \quad (2c)$$

$$P[Event|x(t)] \leq \epsilon_t \quad (2d)$$

$$\bar{x} \leq x \leq \underline{x} \qquad \bar{u} \leq u \leq \underline{u} \qquad \bar{y} \leq y \leq \underline{y} \quad (2e)$$

Bayesian update (time step t out of prediction horizon k)

$$P[Event|x(t+1)] = L\left(x(t)\right) * P[Event|x(t)] \quad (2f)$$

where P is terminal weight, QR and R are controller weights, OH and CH are output and control horizons, N represents the terminal step of the prediction horizon, superscript R is setpoint, t represents the time step for the entire operation of the controller, where at each step, the Bayesian update is applied to refine risk estimates dynamically. The function $f(x_k)$ represents the loss function for safety, which penalizes unsafe behaviors and is formulated based on the specific system under consideration. The details of its selection and impact are discussed in the subsequent section [17] (in (7a)). L is the likelihood function (detailed by [18]). x, y, u represent the state, output and input vectors respectively. Here, x_k corresponds to the system state at prediction horizon k, while $x(t)$ denotes the state at each time step t within the receding horizon framework. The index k represents the prediction step within the optimization window of the receding horizon MPC. At each time step t, the controller solves an optimization problem over the prediction horizon, updating the control inputs accordingly.

$Event$ represents the occurrence of a failure scenario or an undesirable event within the system. It can be defined using mathematical expressions or conditions that capture the event of concern. For instance, in engineering, the event might relate to a variable exceeding a certain threshold. ϵ_t is the threshold value denotes the acceptable level of risk associated with the event. It quantifies the maximum probability at which the event can occur without exceeding acceptable risk levels. The choice of ϵ_t reflects the trade-off between safety and system performance, with lower values indicating a lower tolerance for risk. The probability constraint is handled via chance-constrained programming by obtaining its deterministic approximation [14] (more description in Eqs (5) and (6)).

TANK-LEVEL CONTROL: IMPLEMENTATION, RESULTS & DISCUSSIONS

The proposed R-eMPC framework was applied to the tank-level control system to validate its efficacy in maintaining safety-critical constraints while optimizing performance.

Step 1: High Fidelity Dynamic Modeling

The system dynamics were modeled using mass balance equations, where the liquid level $h(t)$ was regulated by controlling the inlet flow rate $Q_{in}(t)$. The outlet flow rate $Q_{out}(t)$ was assumed proportional to the current liquid level, modeled as $Q_{out}(t) = k\ h(t)$, with k as the proportionality constant. External disturbances $w(t) \sim \mathcal{N}(0{,}0.5)$, were introduced to simulate uncertainties, making the control problem more realistic. The resulting high-fidelity model from Eq. (1) is expressed as follows:

$$\frac{dh(t)}{dt} = \frac{-kh(t)}{A} + \frac{Q_{in}(t)}{A} + \frac{w(t)}{A} \quad (3)$$

Step 2: Model Reduction

To facilitate the design of an optimal control strategy, the high-fidelity dynamic model was simplified into a linear state-space representation. This reduction is typically performed using system identification tools for nonlinear systems to derive an approximate representation that facilitates control design. However, since our system is inherently linear, we can directly express the linear state-space model as:

$$h(i+1) = \left(1 - \frac{k}{A}\right) h(i) + \frac{1}{A} Q_{in}(i) + \frac{1}{A} w(i) \quad (4)$$

Step 3: Risk Modeling via Safety Constraints

Risk modeling was incorporated via probabilistic constraint.

$$P[h(t) > h_{max}] \leq \epsilon_t \quad (5)$$

The probabilistic constraint ensured that the liquid level remained below the maximum allowable height ($h_{max} = 8\ m$) with a predefined risk tolerance (ϵ_t). To ensure computational feasibility, the probabilistic constraint was converted to a deterministic equivalent using chance-constrained programming. Assuming $h(t)$ follows a normal distribution with mean μ_t and standard deviation σ_t, the reformulation yielded:

$$h(t) \leq h_{max} + (z_t \sigma_t) \tag{6}$$

where $z_t = \varphi^{-1}(\epsilon_t)$ represents the z-score corresponding to the risk tolerance, and φ^{-1} is the inverse cumulative distribution function of the standard normal distribution. This deterministic form simplifies the inclusion of the constraint in the optimization problem [14].

Step 4: Risk Informed Explicit Model Predictive Controller

The control objective was to minimize deviations from the setpoint $h_{sp} = 6.4\ m$ while penalizing safety violations using an inverted normal loss function (INLF) [17]. The optimization problem was expressed as:

$$min_u\ J = \sum_{i=1}^{OH-1} \left(\left((h_i - h_{sp})^2 \right) + INLF(h_i, h_{sp}) \right) \tag{7a}$$

s.t.

$$h(i+1) = \left(1 - \frac{k}{A}\right) h(i) + \left(\frac{1}{A}\right) Q_{in}(i) + \left(\frac{1}{A}\right) w(i) \tag{7b}$$

$$0 \leq h(i) \leq h_{max} \tag{7c}$$

$$P(\Delta h > 0|t) \leq \epsilon_t \tag{7d}$$

Bayesian Update:

$$P[\Delta h > 0|t+1] = L(h(t)) * P[\Delta h > 0|t] \tag{7e}$$

Bayesian update is calculated out of the optimization problem before rolling into the next time step in the horizon. The likelihood function being used in Bayesian update is of the functional form that supports the probabilities in the direction of minimal difference between the instantaneous state and the set-point.

$$L(h(t)) = \frac{1}{\sqrt{2\pi}\sigma} \exp\left(-\frac{(h(t) - h_{sp})^2}{2\sigma^2} \right) \tag{7f}$$

The deterministic reformulation of the risk-informed problem is solved using multi-parametric programming, with the initial state h_0 and the parameter $(z_t \sigma_t)$ varying within the range of -3 to +3. This approach enables the explicit computation of control laws as functions of the varying parameters, facilitating efficient real-time implementation while ensuring robust performance under the prescribed risk tolerance. The resulting explicit control map (Figure 2) provide a precomputed map, which can be efficiently used to calculate the optimal solutions for the entire parameter space, ensuring real-time applicability and robust performance under the prescribed risk tolerance [15,16].

The results obtained from the proposed framework provide valuable insights into the behavior and limitations of the control strategies under varying scenarios. Initially, the system was tested with a standard hard-constrained MPC, enforcing the liquid level to strictly adhere to $h(t) \leq h_{max}$. For the first seven-time steps $t = 7$, the controller maintained the liquid level within the permissible range, effectively keeping the system stable. However, as shown in Figure 2, the strict nature of the constraint led to infeasibility at $t = 7$, causing the MPC to fail. Upon failure, the system reverted to an open-loop response, resulting in uncontrolled deviations where the liquid level rapidly exceeded h_{max}. This behavior illustrates the rigidity of hard constraints, which, while effective in maintaining safety under ideal conditions, lack the robustness to handle uncertainty and disturbances effectively.

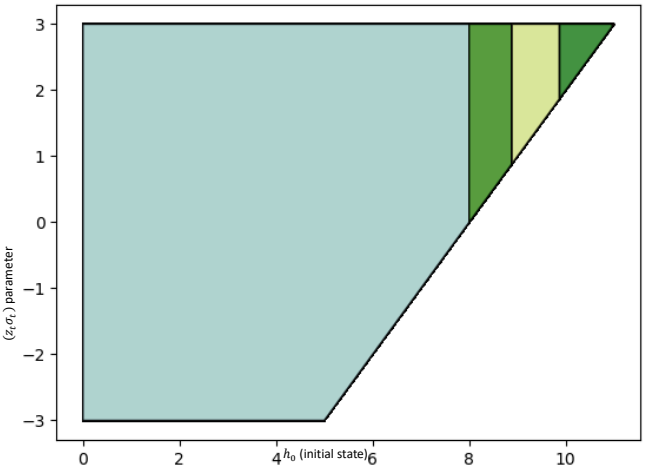

Figure 2. Explicit Control law map of Tank level control

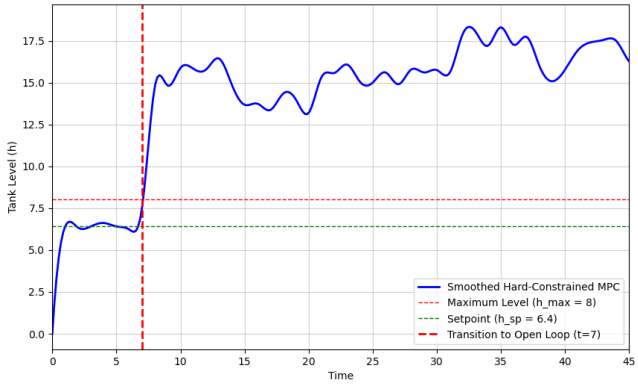

Figure 3. Liquid level evolution under hard-constrained MPC

Recognizing the limitations of a hard-constrained approach, the framework was extended to include probabilistic constraints. By introducing a predefined risk tolerance (ϵ_t), the system gained the ability to handle uncertainties more flexibly. Probabilistic constraints allowed for occasional controlled violations of h_{max} within the acceptable bounds of risk. As depicted in Figure 3, this approach alleviated the infeasibility issues observed with hard constraints, enabling the controller to operate continuously. However, while the liquid level was better

regulated, noticeable excursions beyond h_{max} occurred. These excursions highlight the trade-off inherent in probabilistic constraints: a reduction in controller infeasibility at the expense of occasional deviations beyond safety limits. This raised the need for further refinements to address these excursions effectively.

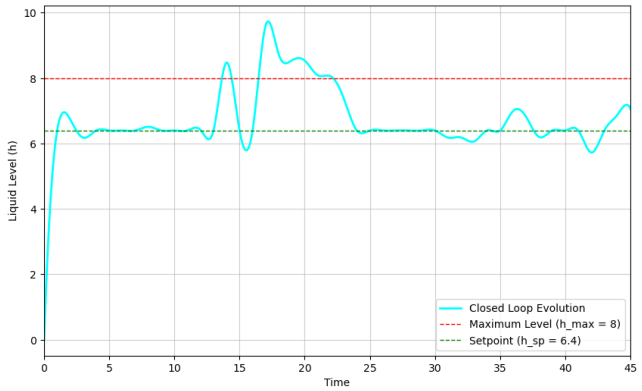

Figure 4. Liquid level evolution under probabilistic constraints

To mitigate the deviations observed in the probabilistic MPC, Bayesian updates and safety-aware objectives were incorporated into the control strategy. Bayesian updates dynamically adapted the risk tolerance (ϵ_t) based on real-time deviations from the setpoint $h_{sp} = 6.4\ m$. The likelihood of deviations was quantified using a functional form that penalized large deviations while favoring adherence to the setpoint. Simultaneously, safety losses were added to the objective function to ensure a direct penalty for violations of h_{max}, effectively steering the system toward safer operation.

The effectiveness of this enhanced framework is evident in Figure 4, where the liquid level remained closer to h_{sp}, with significant reductions in excursions beyond h_{max}. Notably, when deviations beyond h_{max} did occur, the system rapidly adapted its behavior, a capability driven by the dynamic nature of the Bayesian updates. This is further supported by the risk tolerance evolution shown in Figure 5, where ϵ_t sharply decreased during periods of significant deviations, indicating increased caution, and subsequently recovered as the system stabilized. This adaptive response underscores the robustness of the framework in balancing performance and safety under uncertainty.

The comparison of the control strategies highlights the progressive improvement offered by each enhancement. The transition from hard-constrained MPC to probabilistic constraints reduced infeasibility but introduced the challenge of controlling safety violations. The integration of Bayesian updates and safety-aware objectives addressed these challenges by dynamically adapting risk tolerance and penalizing safety violations, ensuring compliance with safety requirements while optimizing system performance. Together, these results demonstrate the proposed R-eMPC framework's ability to provide a robust, adaptive, and computationally efficient solution for managing safety-critical systems under uncertain environments.

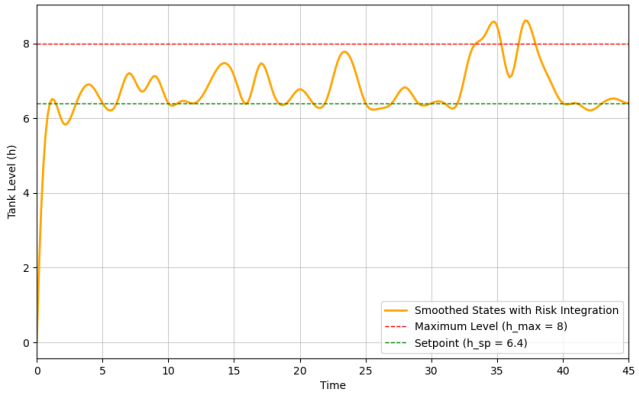

Figure 5. Liquid level evolution with Bayesian updates and safety losses

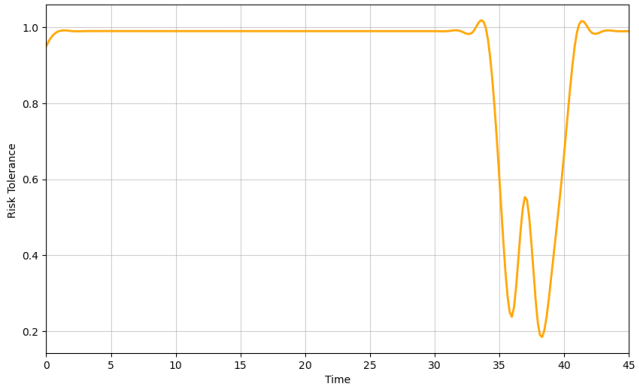

Figure 6. Risk tolerance evolution under Bayesian updates

CONCLUDING REMARKS

In conclusion, the proposed R-eMPC framework demonstrated its efficacy in addressing the critical challenges associated with balancing safety and performance in a safety-critical system under uncertainty. Through a structured progression of enhancements, starting with a conventional hard-constrained MPC, we identified its inherent limitations in handling disturbances and uncertainties, which resulted in system infeasibility and subsequent failure.

By introducing probabilistic constraints, the framework gained flexibility, allowing for controlled risk while maintaining continuous operation. However, the excursions beyond the safety limit highlighted the need for further refinement. The incorporation of Bayesian updates and safety-aware objectives marked a significant step forward, dynamically adapting risk tolerance in real time and penalizing safety violations directly in the objective function. This adaptive capability resulted in substantial

improvements, as the system successfully managed uncertainties while keeping safety-critical constraints in check.

The results underline the importance of incorporating probabilistic considerations and adaptive mechanisms in modern control frameworks. The R-eMPC approach not only mitigated infeasibility but also demonstrated robustness and resilience in handling uncertain conditions, ultimately maintaining safety and improving operational efficiency. These findings highlight the potential of the proposed framework as a powerful tool for safety-critical applications, paving the way for future advancements in adaptive and uncertainty-aware control methodologies.

ACKNOWLEDGEMENTS

The authors acknowledge financial support from NSF RETRO Project CBET-2312457 Texas A&M Energy Institute, Mary O'Connor Process Safety Center and Energy Institute at Texas A&M University and Department of Chemical and Biomedical Engineering at West Virginia University.

REFERENCES

1. Crowl, D. A., & Louvar, J. F. (2001). Chemical process safety: fundamentals with applications. Pearson Education.
2. Kadri, S., Peters, G., VanOmmeren, J., Fegley, K., Dennehy, M., & Mateo, A. (2014). So we all have been implementing process safety metrics—what next?. Process Safety Progress, 33(2), 172-178.
3. Khan, F. I., & Abbasi, S. A. (2000). Towards automation of HAZOP with a new tool EXPERTOP. Environmental Modelling & Software, 15(1), 67-77.
4. Venkatasubramanian, V. (2011). Systemic failures: challenges and opportunities in risk management in complex systems. AIChE Journal, 57(1), 2-9.
5. Pistikopoulos, E. N., Akundi, S. S., Kenefake, D., & Diangelakis, N. A. (2024). The quest towards the integration of process control, process operations, and process operability–Industrial need or academic curiosity?. *Computers & Chemical Engineering*, *180*, 108470.
6. Mayne, D. Q., Rawlings, J. B., Rao, C. V., & Scokaert, P. O. (2000). Constrained model predictive control: Stability and optimality. Automatica, 36(6), 789-814.
7. Aswani, A., Gonzalez, H., Sastry, S. S., & Tomlin, C. (2013). Provably safe and robust learning-based model predictive control. Automatica, 49(5), 1216-1226
8. Akundi, S. S., Braniff, A., Dantas, B., Liu, Y., Tian, Y., Niknezhad, S. S., ... & Pistikopoulos, E. N. (2024). Advanced system control strategies for enhanced safety and efficiency of energy systems. In *Methods in Chemical Process Safety* (Vol. 8, pp. 243-260). Elsevier.
9. Albalawi, F., Durand, H., Alanqar, A., & Christofides, P. D. (2018). Achieving operational process safety via model predictive control. Journal of Loss Prevention in the Process Industries, 53, 74-88.
10. Rivotti, P., Lambert, R. S., & Pistikopoulos, E. N. (2012). Combined model approximation techniques and multiparametric programming for explicit nonlinear model predictive control. Computers & Chemical Engineering, 42, 277-287.
11. Ali, M., Cai, X., Khan, F. I., Pistikopoulos, E. N., & Tian, Y. (2023). Dynamic risk-based process design and operational optimization via multi-parametric programming. Digital Chemical Engineering, 7, 100096.
12. Kalantarnia, M., Khan, F., & Hawboldt, K. (2009). Dynamic risk assessment using failure assessment and Bayesian theory. Journal of Loss Prevention in the Process Industries, 22(5), 600-606.
13. Pistikopoulos, E. N., Diangelakis, N. A., & Oberdieck, R. (2020). Multi-parametric optimization and control. John Wiley & Sons.
14. Ismail, M., El-Hefnawy, A., & Saad, A. E. N. (2018). New deterministic solution to a chance constrained linear programming model with Weibull random coefficients. Future Business Journal, 4(1), 109-120.
15. Pistikopoulos, E. N., Diangelakis, N. A., & Oberdieck, R. (2020). *Multi-parametric optimization and control*. John Wiley & Sons.
16. Kenefake, D., Akundi, S. S., & Pistikopoulos, E. N. A Partial Multiparametric Programming method for Model Predictive Control.
17. Hashemi, S. J., Ahmed, S., & Khan, F. (2014). Loss functions and their applications in process safety assessment. *Process Safety Progress*, *33*(3), 285-291.
18. Amin, M. T., Khan, F., & Imtiaz, S. (2019). Fault detection and pathway analysis using a dynamic Bayesian network. *Chemical Engineering Science*, *195*, 777-790.