Chapter 1

An Operability-based Approach for Integrated Process Design, Operations, and Risk Management

Beatriz Dantas[1], Austin Braniff[1], Sahithi S. Akundi[2,3,4], Yuanxing Liu[2,3,4], Shayan S. Niknezhad[3], Faisal Khan[2,4], Efstratios N. Pistikopoulos[2,3], Fernando V. Lima[1], Yuhe Tian[1*]

[1] Department of Chemical and Biomedical Engineering, West Virginia University
[2] Artie McFerrin Department of Chemical Engineering, Texas A&M University
[3] Texas A&M Energy Institute, Texas A&M University
[4] Mary Kay O'Connor Process Safety Center, Artie McFerrin Department of Chemical Engineering, Texas A&M University

ABSTRACT

The chapter introduces an integrated approach for process design, operations and risk management through operability analysis. Quantitative risk index is integrated with steady-state and dynamic operability analyses using a hierarchical methodological approach to examine the influence of process design, system dynamics, and operating strategies. A safe operating region is identified systematically by mapping available input variables (e.g., design and operational decisions) onto achievable outputs (e.g., process specifications, risk index), which leads to minimizing risks while improving the overall process efficiency. By integrating safety considerations into the conceptual design phase, the study contributes to develop robust and reliable chemical processes that can withstand operational uncertainties and disturbances. The proposed approach is demonstrated through a case study on an exothermic continuous stirred-tank reactor producing gasoline additive as motivated by a process safety incident at T2 Laboratories Inc.

KEYWORDS

Process Operability, Risk Analysis, Design Optimization, Operation under Uncertainty

* Corresponding author.
E-mail address: yuhe.tian@mail.wvu.edu (Y. Tian).

1.1 INTRODUCTION

Process Safety Management (PSM) aims to prevent the occurrence of hazardous chemical incidents, which is key for the sustainable development of chemical and energy industries from all the aspects of environment, society, and economics [1,2]. A cohesive PSM approach is thus crucial to ensure safe, efficient, and environmentally friendly processes by integrating design, manufacturing, and sustainable engineering considerations. Toward this direction, risk analysis offers a quantitative method to assess process safety performance and to prevent accidents from occurring or recurring [3,4]. A representative application of risk analysis is to minimize shutdown times and decrease production losses by maintaining high equipment availability, thereby ensuring the overall profitability [5]. These assessments should be performed throughout the process development stages from steady-state design optimization, control system design, to real-time operation to consistently enhance process safety and reliability at the minimal cost [6–8].

Process operability analysis has become an instrumental tool in achieving the integration of process design, control, and operations. It systematically identifies the feasible operating window through comprehensive model-based analyses of operational uncertainties, disturbances, and constraint violations [9]. At steady state, process operability analysis was successfully demonstrated to design nonlinear process systems such as that presented in Carrasco and Lima [10] for modular and intensified energy systems. The operability concepts were also applied to investigate the feasibility of emerging membrane technologies for direct air capture [11]. While steady-state operability analysis focuses on characterizing the feasibility of a process design, dynamic operability evaluates real-time operations as a function of time. A dynamic operability index [12] was defined to assess system performance across the desired output and expected disturbance ranges. This index could identify bottlenecks caused by input limitations and provide guidance on adjusting input ranges to enhance process operability. Furthermore, the concept of output funnels was introduced to dynamic systems based on the steady-state interval operability approach [13]. The analysis served as an initial step to verify the feasibility of control objectives throughout the entire control horizon. A more recent work [14] illustrated the intricate relationships among process design, control structure, and control law with application to a modular process. A closed-loop control metric was also introduced to compare the performance of various operable designs. The above operability concepts have been integrated as an open-source Python Opyrability package which is publicly available to the community [15].

However, an open research question remains on how to integrate process safety considerations with operability analysis. Operability analysis offers the potential to identify the safe steady-state design space and dynamic operating window prior to operating the process online while accounting for plausible disturbances. To address the gap, this study introduces an integrated approach that

combines process design, operations, and risk optimization through operability analysis. The proposed approach aims to enhance the overall process safety performance by characterizing the feasibility of a safe operating region, thus offering guidance for process design and operational strategies. The risk index developed by Bao et al. [16] is utilized to quantify process safety during both steady state and dynamic operations. A case study is presented to demonstrate the integrated approach, focusing on an exothermic continuous stirred-tank reactor (CSTR) used in the production of a gasoline additive. The case study is based on a major process safety accident at T2 Laboratories Inc. [17,18].

The remainder of this chapter is organized as follows: Section 1.2 introduces a hierarchical approach for process design, operations, and risk management. Section 1.3 demonstrates the method on an exothermic reactor encompassing both steady-state and dynamic scenarios. Section 1.4 discusses concluding remarks and ongoing work.

1.2 METHODOLOGY: AN OPERABILITY-BASED APPROACH FOR RISK MANAGEMENT

The integrated approach proposed for this study features the following major steps to enhance operability and safety:

1. Process and risk modeling of the safety-critical system.
2. Integrating risk index into steady-state operability-based process design.
3. Incorporating dynamic operability and risk analyses to enhance process operational safety.

Step 1: Process and risk modeling of the safety-critical system.

A process model is first developed to mathematically describe the mechanistic and/or data-driven relationships between the process state, output, and input variables (including both manipulated variables and disturbances). A generic form of the process model M is shown in Equation (1.1).

$$M = \begin{cases} \dot{x} = f(x, u, d) \\ y = g(x, u, d) \\ h_1(\dot{x}, x, y, \dot{u}, u, d) = 0 \\ h_2(\dot{x}, x, y, \dot{u}, u, d) \geq 0 \end{cases} \tag{1.1}$$

where $x \in \mathbb{R}^n$ represents the vector of state variables with a dimension of n, $y \in \mathbb{R}^p$ denotes the vector of outputs, $u \in \mathbb{R}^m$ stands for the vector of inputs, and $d \in \mathbb{R}^q$ represents the vector of disturbances. The functions $f : \mathbb{R}^{m+n+q} \rightarrow \mathbb{R}^n$ and $g : \mathbb{R}^{m+n+q} \rightarrow \mathbb{R}^p$ describe nonlinear mappings. The constraints h_1 and h_2 correspond to equality and inequality process constraints, respectively. Additionally, $\dot{x}$ and $\dot{u}$ indicate the time derivatives associated with x and u, respectively. For steady-state analysis, the time derivatives take the value of 0.

On this basis, the risk model can be developed as a function of the safety-critical process variables following the strategy presented in [16]. In what follows, we use x to denote the safety-critical process variables (e.g., states) without loss of generality. The risk index RI is formulated based on the deviation of x from the nominal design or operating conditions (μ). Equation (1.2) defines RI as the product of fault probability $P(x)$ and consequence severity $S(x)$. It is worth highlighting that Equation (1.2) can be applied for both static and dynamic risk analysis, respectively, using the steady-state values x_{ss} or described as a function of time $x(t)$. More detail on the application of RI for real-time risk monitoring and management can be found in Ali et al. [18].

$$RI = P(x) \times S(x) \tag{1.2}$$

Fault Probability

The fault probability is determined using Equation (1.3), which uses the probability density function defined in relation to the mean (μ) and standard deviations (σ) of the safety-critical process variables (x). The three-sigma rule ($\mu \pm 3\sigma$) is utilized in this definition. As per statistics, approximately 99.7% of the values lie within three standard deviations of the mean. In this way, the resulting risk calculation particularly emphasizes the potential abnormality incurred by the process departure from the three-sigma region as showcased in Figure 1.1.

$$P(x) = \begin{cases} \phi\left[\frac{x-(\mu+3\sigma)}{\sigma}\right] = \int_{-\infty}^{x} \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{[t-(\mu+3\sigma)]^2}{2\sigma^2}} dt, & \text{when } x \geq \mu \\ \phi\left[\frac{x-(\mu-3\sigma)}{\sigma}\right] = \int_{-\infty}^{x} \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{[t-(\mu-3\sigma)]^2}{2\sigma^2}} dt, & \text{when } x < \mu \end{cases} \tag{1.3}$$

Consequence Severity

The consequence severity term accounts for the potential hazard caused by the deviation of the safety-critical process variables, x. Equation (1.4) is utilized to quantify the severity of the fault, a measure that escalates significantly as the deviation of x from the nominal operating point increases.

$$S(x) = \begin{cases} 100^{\frac{x-(\mu+3\sigma)}{x-\mu}}, & \text{when } x \geq \mu \\ 100^{\frac{(\mu-3\sigma)-x}{\mu-x}}, & \text{when } x < \mu \end{cases} \tag{1.4}$$

Step 2: Integrating risk index into steady-state operability-based process design.

Based on the process and risk model developed in Step 1, a steady-state operability analysis is conducted, which quantifies the ability of a process to maintain feasible functionality under disturbances. This step only evaluates the feasibility of the transition between steady states, while Step 3 further takes the dynamic

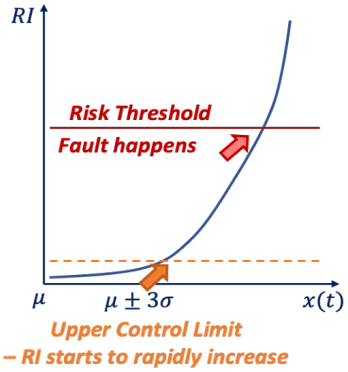


FIGURE 1.1 Risk modeling.

transition path into account. Using the notation described above, we can define the following basic operability sets as introduced in Gazzaneo et al. [9]. Figure 1.2 depicts a schematic of process operability concepts. Of particular interest to this work is the risk index RI, which is incorporated as one of the output variables. A desired output set can be defined and tailored to the required risk index level (e.g., $RI \leq 0.1$). The process inverse mapping procedure can then systematically identify the maximum disturbance rejection region and the corresponding design and operational input regions (i.e., desired input set), which ensure the achievement of the desired process safety performance. This step serves as the first-round screening to obtain the feasible design, operating, and disturbance region with acceptable risks, which provides the superset for the next step, dynamic operability analysis [19].

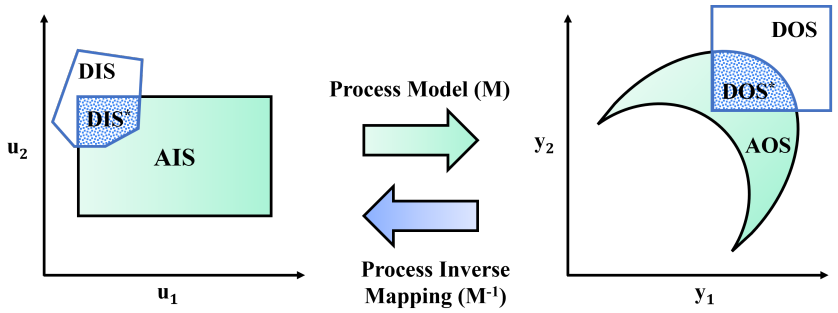


FIGURE 1.2 Schematic of the process operability concepts.

Available Input Set (AIS): This set represents the operational variables (e.g., flow rates of reactants, temperatures, and pressures) and/or design specifications (e.g., equipment dimensions, catalyst type, and loading) of a process system.

Mathematically, the AIS is given in Equation (1.5).

$$\text{AIS} = \left\{u \in \mathbb{R}^m \mid u^{\min} \leq u \leq u^{\max}\right\} \tag{1.5}$$

Expected Disturbance Set (EDS): This set represents the expected steady-state values of disturbances, as defined in Equation (1.6). Additionally, this set can account for process uncertainties in the model parameters used in the design.

$$\text{EDS} = \left\{d \in \mathbb{R}^q \mid d^{\min} \leq d \leq d^{\max}\right\} \tag{1.6}$$

Achievable Output Set (AOS): This set encompasses the output variables that the system can achieve, considering both the available input set (AIS) and the expected disturbance set (EDS). Typically, it is defined in terms of inputs and disturbances. For each disturbance d, the Achievable Output Set (AOS) is defined as shown in Equation (1.7).

$$\text{AOS}_u(d) = \{y \in \mathbb{R}^p \mid y = M(u, d) \text{ and } u \in \text{AIS}, d \in \text{EDS}\} \tag{1.7}$$

Desired Output Set (DOS): This set outlines the desired operational ranges in terms of outputs. The boundaries of this set are determined by process constraints and/or considerations regarding the desired process production and efficiency. Mathematically, it is expressed as Equation (1.8). The DOS^*, as shown in Figure 1.2, indicates the intersection of AOS and DOS, representing the feasible operating region.

$$\text{DOS} = \left\{y \in \mathbb{R}^p \mid y^{\min} \leq y \leq y^{\max}\right\} \tag{1.8}$$

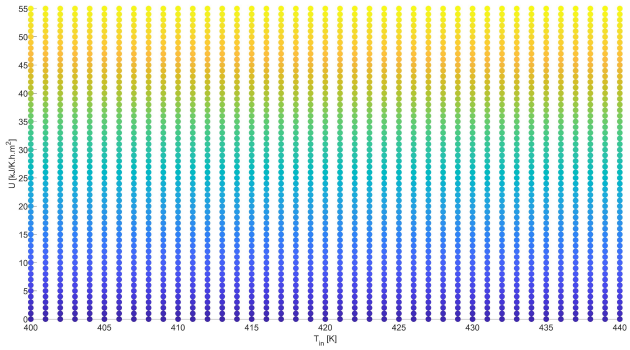
Desired Input Set (DIS): This set comprises the required inputs needed to achieve the entire DOS via an inverse mapping (M^{-1}). Similarly, the DIS^* shown in Figure 1.2 indicates the intersection of AIS and DIS, representing the feasible input region. Equations (1.9) describe scenarios where disturbances d are considered.

$$\text{DIS}_y(d) = \left\{u \in \mathbb{R}^m \mid M^{-1}(y, d) \text{ and } y \in \text{DOS}, d \in \text{EDS}\right\} \tag{1.9}$$

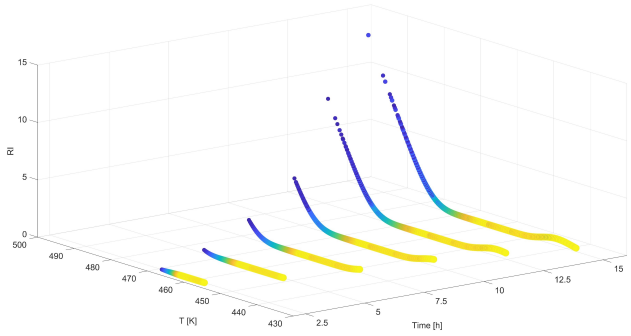
Step 3: Incorporating dynamic operability and risk analyses to enhance process operational safety.

Dynamic operability aims to assess the feasibility of time-varying operations, determining whether the manipulated variables can sufficiently counteract the effects of disturbances during transient. It follows the same operability concepts defined for steady-state analysis (AIS, AOS, etc.) while taking the time domain into consideration, as depicted in Figure 1.3. This work performs an open-loop dynamic operability analysis, which helps to understand the system's time-dependent response and guides the selection of closed-loop control strategies for

disturbance rejection. The ultimate objective is to identify potential operating windows, namely the lower and upper bounds of operating variables, that can maintain operations at an acceptable risk level despite disturbances.



(a) Available Input Set (AIS)



(b) Achievable Output Set (AOS)

FIGURE 1.3 Dynamic Operability Analysis.

1.3 CASE STUDY: T2 CSTR RISK MANAGEMENT

1.3.1 Process Description

Reactive chemical hazards are critical to process safety, as they include the potential risks that emerge from chemical interactions. Neglecting these risks can lead to major accidents such as fire, explosions, or the release of toxic substances [20]. The CSTR process investigated in this work was involved in a tragic explosion that occurred on December 19, 2007, at T2 Laboratories in Jacksonville, Florida. This incident resulted in four people being killed and

32 injured [17]. The facility was producing methylcyclopentadienyl manganese tricarbonyl, an Ecotane brand gasoline additive, in a 2500-gallon batch reactor. In this study, the CSTR depicted in Figure 1.4 is operated under conditions similar to those of the original T2 batch reactor studied in literature [18,21]. This process involves two feed streams to the CSTR: one containing reactant A in solvent S and the other containing reactant B. Both feed streams are preheated before entering the reactor.

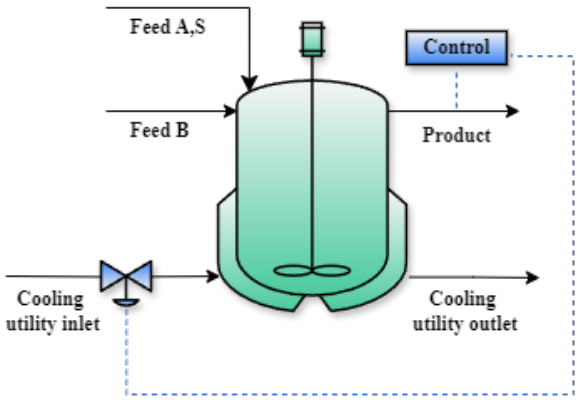


FIGURE 1.4 The T2 CSTR process.

During the initial production step, the explosion was triggered by a large reactor vessel bursting due to a runaway reaction. Such thermal runaway happens when the process fails to remove sufficient heat from the reactor to regulate the temperature. As a result, the reactor temperature rises, leading to an accelerated reaction rate and even faster heat generation, as shown in Figure 1.5. Thus, the reactor temperature (T) is chosen as the safety-critical process variable in this study, with a setpoint of 460 K (i.e., nominal operating condition), subject to fluctuations in feed inlet temperature (i.e., disturbance). The high-risk region is defined based on $T \geq 480$ K, with a higher probability of thermal runaway occurring. The two exothermic reactions involved in this reactor vessel are given below, where the second reaction becomes significant only at elevated temperatures.

$$\begin{aligned} &\text{Reaction 1: Methylcyclopentadiene (A) + Sodium (B)} \\ &\xrightarrow{\text{Diglyme } (S)} \text{Sodium Methylcyclopentadiene (C) + Hydrogen (D)} \\ &\text{Reaction 2: Diglyme (S)} \xrightarrow{\text{Sodium } (B)} \text{Hydrogen (D) + Byproduct} \end{aligned} \tag{1.10}$$

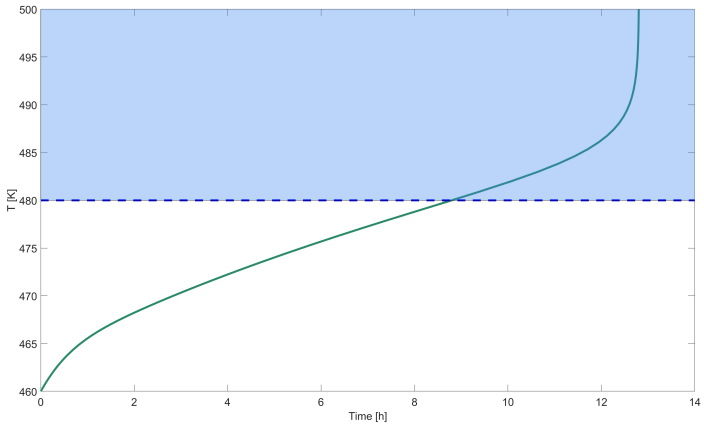


FIGURE 1.5 T2 CSTR open-loop simulation.

The specific research objectives of this case study are summarized below:

1. Reactor process and risk modeling: A first principles model is developed to mathematically describe the above reactor comprising mass/energy balances and reaction kinetics. The reactor temperature is chosen as the safety-critical process variable based on the risk index definition.
2. Steady-state operability analysis for process design with risk considerations: Process design and operating regions are identified, potentially leading to low, medium, and high risks under uncertainties. It allows for the quantification of risks while ensuring process operability.
3. Dynamic operability and risk analyses to enhance operational safety: System dynamics is incorporated to analyze the open-loop behavior of the CSTR under disturbances. The results help to define the safely feasible operating ranges and transition paths to guide controller design.

1.3.2 Reactor Modeling and Simulation

The first principles model assumes an ideal CSTR with constant volume [18]. The dynamic mass balances for reactants A, B, and S are given in Equations (1.11), (1.12) and (1.13). The dynamic energy balance in the reactor vessel is given in Equation (1.14). The reaction rate expressions are presented in Equation (1.15) and the CSTR parameter definitions in Table 1.1. The risk is modeled as per Equations 1.3 and 1.4 with the mean (μ) as 460 K and standard deviation (σ) as 5 K. This gives the three-sigma region ($\mu + 3\sigma$) up to 475 K. As introduced in Section 1.2, the risk will rapidly escalate between 475 K (upper control limit) and 480 K (high-risk region), thus emphasizing the urgency for risk management.

The risk levels are defined as follows: (i) low-risk ($RI \approx 0$) – reactor temperature around the nominal condition, (ii) medium-risk ($RI = 0.74$) – reactor at upper control limit, (iii) high-risk ($RI = 2.82$) – reactor has high probability of thermal runaway, for which emergency shutdown is required.

$$\frac{dC_A(t)}{dt} = \frac{F_{A,\,\text{in}}}{V} - \frac{q_{\text{out}}}{V} C_A(t) - k_1(T(t)) C_A(t) C_B(t) \tag{1.11}$$

$$\frac{dC_B(t)}{dt} = \frac{F_{B,\,\text{in}}}{V} - \frac{q_{\text{out}}}{V} C_B(t) - k_1(T(t)) C_A(t) C_B(t) \tag{1.12}$$

$$\frac{dC_S(t)}{dt} = \frac{F_{S,\,\text{in}}}{V} - \frac{q_{\text{out}}}{V} C_S(t) - k_2(t) C_S(t) \tag{1.13}$$

$$\frac{dT(t)}{dt} = \frac{q_{\text{out}}}{V} \left(T_{\text{in}}\,(t) - T(t)\right) + \frac{\sum \left(-\Delta H_k\right) r_k(t)}{\rho c_p} - \frac{U A_x \left(T(t) - T_c\right)}{\rho c_p V} \tag{1.14}$$

$$\begin{aligned} &\text{Reaction 1: } r_1 = -k_1 C_A C_B, \text{ where } k_1 = k_{10} \exp\left(-\frac{E_1}{RT}\right) \\ &\text{Reaction 2 : } r_2 = -k_2 C_S, \text{ where } k_2 = k_{20} \exp\left(-\frac{E_2}{RT}\right) \end{aligned} \tag{1.15}$$

TABLE 1.1 List of CSTR process parameters.

Variable	Description	Value	Unit
$F_{A,\,\text{in}}$	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}	l/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

1.3.3 Steady-State Analysis

For steady-state operability analysis, the AIS includes a single manipulated variable, i.e., the heat transfer coefficient U as the simplification from using the cooling utility flowrate, which ranges from 0 to 55 $\mathrm{kJ}/\left(\mathrm{K}\cdot\mathrm{h}\cdot\mathrm{m}^2\right)$. The EDS comprises one disturbance variable, the feed inlet temperature T_{in}, which ranges from 400 to 440 K. The resulting AOS is characterized by the risk index RI, which depends on the outlet temperature (T). Selecting a broad operating range during the design phase can holistically identify the feasible operational regions with respect to all levels of risk, thereby facilitating proactive risk management in the safety-critical system.

In this case study, the forward mapping of the AIS, taking into account the EDS, is obtained by discretizing the entire sets. Figure 1.6 shows the operability mapping. The analysis results indicate that high-risk regions can be avoided by selecting good steady-state design/operating conditions for U. As depicted, at steady state, the risk should not exceed the threshold that triggers the thermal runaway risk (RI $\geq$ 2.82). The maximum disturbance tolerance can thus be quantified using this figure with respect to each U value. For example, if the steady-state value of U is designed as 5 $\mathrm{kJ}/\left(\mathrm{K}\cdot\mathrm{h}\cdot\mathrm{m}^2\right)$, the maximum disturbance that can be accommodated is T_{in} around 427 K to avoid high-risk operations. However, if U = 35 $\mathrm{kJ}/\left(\mathrm{K}\cdot\mathrm{h}\cdot\mathrm{m}^2\right)$, operations are not expected to be at high risk within the entire disturbance set.

As highlighted by the red box in Figure 1.6, the reactor will enter the medium-to-high risk region ($0.74 \leq RI \leq 2.82$) when the heat transfer coefficient at steady state is designed between 0 to 35 $\mathrm{kJ}/\left(\mathrm{K}\cdot\mathrm{h}\cdot\mathrm{m}^2\right)$ under elevated inlet temperature disturbances (T_{in} ranging from 415 K to 440 K). On the other hand,

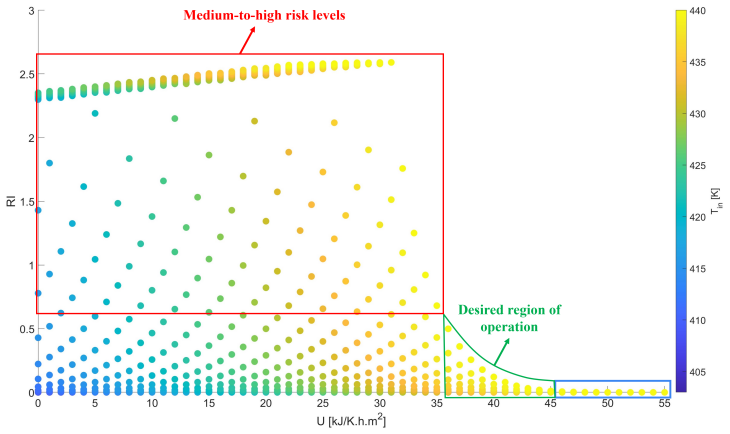


FIGURE 1.6 Joint input-output plot with respect to RI for $x \geq \mu$.

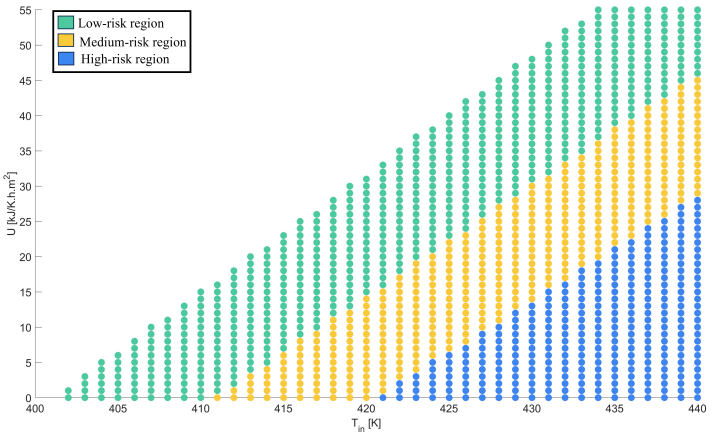
if a large heat transfer coefficient value is used, 45 to 55 $\mathrm{kJ}/\left(\mathrm{K}\cdot\mathrm{h}\cdot\mathrm{m}^2\right)$, the reactor can be constantly operated at a very low-risk level despite the expected disturbances, as shown by the blue box. However, higher heat transfer coefficient values also indicate more cooling utility use, which may present a trade-off solution for safety and economics. Given this, the preferable steady-state values for U is 35 to 45 $\mathrm{kJ}/\left(\mathrm{K}\cdot\mathrm{h}\cdot\mathrm{m}^2\right)$, which is sufficient to maintain low-to-medium risk levels ($RI \leq 0.74$) even at the highest disturbance value (440 K) while requiring fewer cooling water resources. Thus, using the proposed method, the steady-state operability calculations are able to provide a systematic map of all input and disturbance variable combinations, identifying configurations that could potentially enhance the system's safety at the early design stage.

1.3.4 Dynamic Analysis

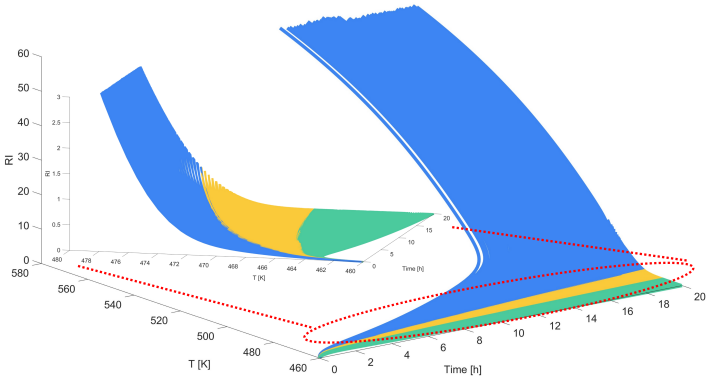
Evaluating steady-state operability is an important initial step that should be followed by examining dynamic operability to incorporate the impact of system dynamics. In this dynamic study, the input variables, i.e. the manipulated variable U and disturbance T_{in}, are assumed to remain constant from the initial to the final time while the reactor operates dynamically. This assumption simplifies the analysis by eliminating the variability and uncertainty arising from potential changes in input variables, allowing us to focus on the intrinsic dynamics of the system. This scenario also serves as the baseline for more complex cases to be investigated in future work where inputs and disturbances vary over time. The ranges for manipulated and disturbance variables are the same as those considered in the steady-state analysis. Figure 1.7 shows the analysis results categorizing three distinct operating regions based on the risk levels. The first region, shown in green ($RI \leq 0.00175$), involves effective operations at low-risk levels. The second region, represented in yellow ($RI \leq 0.74$), corresponds to medium-risk levels. The third region, depicted in blue, pertains to high-risk levels, as discussed in [18].

The AIS and EDS are depicted in Figure 1.7(a), and the AOS is shown in Figure 1.7(b). The highlighted high-risk region (in blue) supports the steady-state observation that a thermal runaway is triggered by higher inlet temperatures, causing a greater interruption to the system. This interruption results in a significant increase in reactor temperature due to the nature of exothermic reactions exacerbated by inadequate cooling. Avoiding this region is crucial for safe operation. The medium-risk region comprises regions beyond $\mu + 3\sigma$, presented in yellow, which shows a rapid increase in risk as it further departs from the upper control limit. This marks a step closer to the high-risk region, where the temperature becomes increasingly challenging to control, potentially leading to thermal runaway. Finally, the low-risk region, depicted in green, encompasses a range of values from the lowest to the highest manipulated variable values and disturbance levels. This region represents all possible combinations of manipulated and disturbance variables that enable effective control while ensuring low

risk. Operating the reactor around a well-controlled low-to-medium risk level may be a preferable trade-off solution as it may render lower economic costs without compromising the process safety performance. This analysis not only provides insights into how the system behaves over time but also helps us understand the dynamic transient behavior leading to steady states (or set points), hence offering valuable insights for process control and safety considerations.



(a) Available Input Set (AIS)



(b) Achievable Output Set (AOS)

FIGURE 1.7 Dynamic Operability Analysis for $x(t) \geq \mu$.

1.4 CONCLUSIONS AND ONGOING WORK

In this chapter, a novel approach has been introduced to integrate process design, operations, and risk optimization by incorporating safety through process operability. This approach facilitated risk assessment by quantitatively accounting for the impact of design and/or operational variables on process safety. This approach offers the potential to proactively circumvent abnormal conditions associated with these processes, starting from the early design stage, by integrating safety metrics into the classic process operability concepts. The effectiveness of the developed approach was demonstrated through a case study involving an exothermic CSTR, motivated by a major process safety accident at T2 Laboratories Inc. caused by a thermal runaway. The steady-state analysis systematically explored all combinations of input and disturbance variables that remained below the threshold to prevent triggering the fault of thermal runaway. The design space, which may lead to high process risk, has also been identified. Dynamic process operability was assessed under constant input variable profiles while the reactor operated dynamically. This analysis quantified low, medium, and high-risk regions, showcasing all possible combinations within the available input set that enable effective control while ensuring safety. This dynamic mapping demonstrated the system's behavior in an open-loop scenario and identified the regions characterized as a safe operating interval with respect to the manipulated variable and disturbance levels. The ongoing work involves developing the dynamic mapping strategy for closed-loop controller design, which enables the leverage of a multi-parametric model predictive controller for optimal risk management.

ACKNOWLEDGMENTS

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

DECLARATION OF AI AND AI-ASSISTED TECHNOLOGIES IN THE WRITING PROCESS

During the preparation of this work the author(s) used ChatGPT 3.5 in order to improve readability. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the publication.

REFERENCES

[1] W. Nawaz, P. Linke, M. Koc, Safety and sustainability nexus: A review and appraisal, Journal of Cleaner Production 216 (2019) 74–87.

[2] E. N. Pistikopoulos, Y. Tian, Advanced modeling and optimization strategies for process synthesis, Annual Review of Chemical and Biomolecular Engineering 15 (2024).

[3] Center for Chemical Process Safety, Guidelines for risk based process safety, John Wiley & Sons, 2011.

[4] F. I. Khan, P. R. Amyotte, M. T. Amin, Advanced methods of risk assessment and management: An overview, Methods in chemical process safety 4 (2020) 1–34.

[5] A. Hameed, F. Khan, A framework to estimate the risk-based shutdown interval for a processing plant, Journal of Loss Prevention in the Process Industries 32 (2014) 18–29. doi:10.1016/j.jlp.2014.07.009.

[6] K. G. Lough, R. B. Stone, I. Tumer, Implementation procedures for the risk in early design (red) method, Journal of Industrial and Systems Engineering 2 (2008) 126–143.

[7] S. Park, S. Xu, W. Rogers, H. Pasman, M. M. El-Halwagi, Incorporating inherent safety during the conceptual process design stage: A literature review, Journal of Loss Prevention in the Process Industries 63 (2020) 104040. doi:10.1016/j.jlp.2019.104040.

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

[9] V. Gazzaneo, J. C. Carrasco, D. R. Vinson, F. V. Lima, Process Operability Algorithms: Past, Present, and Future Developments, Industrial and Engineering Chemistry Research 59 (2020) 2457–2470. doi:10.1021/acs.iecr.9b05181, publisher: American Chemical Society.

[10] J. C. Carrasco, F. V. Lima, An optimization-based operability framework for process design and intensification of modular natural gas utilization systems, Computers and Chemical Engineering 105 (2017) 246–258. doi:10.1016/j.compchemeng.2016.12.010, publisher: Elsevier Ltd.

[11] V. Gama, B. Dantas, O. Sanyal, F. V. Lima, Process Operability Analysis of Membrane-Based Direct Air Capture for Low-Purity CO_2 Production, ACS Engineering Au (2024) acsengineeringau.3c00069. doi:10.1021/acsengineeringau.3c00069.

[12] D. Uztürk, C. Georgakis, Inherent dynamic operability of processes: General definitions and analysis of SISO cases, Industrial and Engineering Chemistry Research 41 (2002) 421–432. doi:10.1021/ie0101792, publisher: American Chemical Society.

[13] F. V. Lima, C. Georgakis, Dynamic Operability for the Calculation of Transient Output Constraints for Non-Square Linear Model Predictive Controllers, IFAC Proceedings Volumes 42 (2009) 231–236. doi:10.3182/20090712-4-TR-2008.00035.

[14] S. Dinh, F. V. Lima, Dynamic Operability Analysis for Process Design and Control of Modular Natural Gas Utilization Systems, Industrial & Engineering Chemistry Research 62 (2023) 2052–2066. URL: https://pubs.acs.org/doi/10.1021/acs.iecr.2c03543. doi:10.1021/acs.iecr.2c03543.

[15] V. Alves, S. Dinh, J. R. Kitchin, V. Gazzaneo, J. C. Carrasco, F. V. Lima, Opyrability: A Python package for process operability analysis, Journal of Open Source Software 9 (2024) 5966. URL: https://joss.theoj.org/papers/10.21105/joss.05966. doi:10.21105/joss.05966.

[16] 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. URL: https://aiche.onlinelibrary.wiley.com/doi/10.1002/prs.10421. doi:10.1002/prs.10421.

[17] Chemical Safety Board, T2 laboratories inc. reactive chemical explosion, 2009. URL: https:

//www.csb.gov/t2-laboratories-inc-reactive-chemical-explosion/.

[18] M. Ali, X. Cai, F. I. Khan, E. N. Pistikopoulos, Y. Tian, Dynamic risk-based process design and operational optimization via multi-parametric programming, Digital Chemical Engineering 7 (2023) 100096. URL: https://linkinghub.elsevier.com/retrieve/pii/S2772508123000145. doi:10.1016/j.dche.2023.100096.

[19] E. N. Pistikopoulos, Y. Tian, R. Bindlish, Operability and control in process intensification and modular design: Challenges and opportunities, AIChE Journal 67 (2021) e17204.

[20] D. A. Crowl, Chemical process safety : fundamentals with applications / Daniel A. Crowl, Joseph F. Louvar. (2011). Edition: 3rd ed. Publisher: Prentice Hall.

[21] J. Ariamuthu Venkidasalapathy, C. Kravaris, Safety-centered process control design based on dynamic safe set, Journal of Loss Prevention in the Process Industries 65 (2020) 104126. doi:10.1016/j.jlp.2020.104126.