Contents lists available at ScienceDirect

Chemical Engineering Research and Design

journal homepage: www.elsevier.com/locate/cherd

On integration of feedback control and safety systems: Analyzing two chemical process applications

Zhihao Zhang[a], *Zhe Wu*[a], *Helen Durand*[b], *Fahad Albalawi*[c], *Panagiotis D. Christofides*[a,d,*]

[a] *Department of Chemical and Biomolecular Engineering, University of California, Los Angeles, CA 90095-1592, USA*
[b] *Department of Chemical Engineering and Materials Science, Wayne State University, Detroit, MI 48202, USA*
[c] *Department of Electrical Engineering, Taif University, Taif 21974, Saudi Arabia*
[d] *Department of Electrical and Computer Engineering, University of California, Los Angeles, CA 90095-1592, USA*

ARTICLE INFO

Article history:
Received 11 January 2018
Received in revised form 2 February 2018
Accepted 5 February 2018
Available online 13 February 2018

Keywords:
Model predictive control
Process control
Process safety
Reaction thermal runaway
High-pressure flash drum separator

ABSTRACT

This work focuses on two case studies and attempts to elucidate the dynamic interaction between feedback control and safety systems in the context of both model-based and classical control systems. In the first case study, the interaction of a model predictive control (MPC) system with a safety system is studied in the context of the methyl isocyanate (MIC) hydrolysis reaction in a continuous stirred tank reactor (CSTR) to avoid thermal runaway. We develop a specific action for the MPC to take when the safety system is activated due to significant feed disturbances that lead to thermal runaway conditions. In the second case study, we focus on a high-pressure flash drum separator for which the temperature, level, and pressure can be regulated using proportional-integral (PI) controllers. Using a large-scale dynamic process simulator, we demonstrate that modifying the tuning parameters of one of these PI controllers based on the safety system being on or off leads to improved closed-loop performance compared to the case in which the tuning parameters of the PI controller remain the same regardless of the state of the safety system.

1. Introduction

The continued occurrence of incidents in the chemical process industries, despite efforts to prevent them (Center for Chemical Process Safety, 2008; AIChE, 1994a,b), is a testament to the need for continued work focused on enhancing process operational safety to protect human lives and the environment (Smith et al., 2003). Several recent works have proposed a systems perspective to process safety (e.g., Leveson and Stephanopoulos, 2014; Venkatasubramanian, 2011; Mannan et al., 2015; Albalawi et al., 2016) which encourages engineers to consider process incidents as events that occur due to a migration of the process state, over time, to conditions at which an accident may occur (this may be applicable, for example, in the case of reactor thermal runaway). Traditional approaches to process safety like process design modifications neglect important aspects impacting process operational safety, such as multivariable interactions of process components and variables, limited control system authority due to limitations on the capacity of control actuators, and the manner in which the safety or relief system response may impact the effectiveness of the process control system (Wang et al., 2016; Leveson and Stephanopoulos, 2014). Accounting for such aspects in the control and safety system designs can be crucial to ensuring process operational safety.

* *Corresponding author at*: Department of Chemical and Biomolecular Engineering, University of California, Los Angeles, CA, 90095-1592, USA.
E-mail address: pdc@seas.ucla.edu (P.D. Christofides).
https://doi.org/10.1016/j.cherd.2018.02.009

Some of these issues, such as interactions between process states, can be accounted for using the optimization-based industrial feedback control design termed model predictive control (MPC), which utilizes a process dynamic model to make state predictions that are used in selecting optimal control actions with respect to an objective function (Qin and Badgwell, 2003; Ellis et al., 2014, 2016, 2017; Morari and Lee, 1999; Mayne et al., 2000; Rawlings, 2000; Christofides et al., 2013). In addition, MPC may be augmented with state constraints to limit excursions of the process state into unsafe regions of state-space. However, no MPC design has yet been developed that can account for the activation of the safety system when the process state enters an unsafe operating region due to equipment faults or disturbances. Overall, coordinating the control and safety systems so that the triggering conditions for the elements of the safety system (e.g., alarms, pressure relief devices, and emergency shutdown systems) account for control actuator limitations, and the control system actions account for the activation of the safety system, would represent a significant paradigm shift in both control and safety system design that has the potential to save lives and protect the environment. In California, there have been several high-profile accidents including one in an Exxon refinery in Torrance, Los Angeles in 2015. In this accident, due to malfunction of the emergency systems, major flammable vapor leaks occurred from a pipe at the fluidized catalytic cracker unit that sent thousands to the hospital; this is the type of accident that could have been prevented with coordination of the process control and emergency safety systems such that the control system could safely operate the plant in a limited operation regime until the emergency system was brought back on-line (Marsh, 2016). A critical aspect of any coordination of the control and safety systems is that these systems must remain independent so that failure of one system does not result in failure of the other.

Several works have looked at coordinating control with safety considerations. For example, thresholds on a recently developed state-based Safeness Index (Albalawi et al., 2017) may be incorporated as triggers for safety system activation that allow the safety system to be aware of system-level safety considerations; the same metric, with different thresholds, can be utilized in MPC design to provide some coordination between the designs. Control designs (Mhaskar et al., 2013; Mhaskar, 2006; Lao et al., 2013; Kettunen et al., 2008; Prakash et al., 2002; Bø and Johansen, 2014; Xue and El-Farra, 2016; Allen and El-Farra, 2017) have been developed that can handle safety in the sense of faults (Venkatasubramanian et al., 2003; Çinar et al., 2007; Gajjar and Palazoglu, 2016); however, these methods do not address safety system actions in control. Therefore, the development of systematic methods for coordinating control and safety systems poses fundamental challenges; for example, control/safety system logic should be developed to directly account for the impact of discrete safety system actions (like on/off behavior of relief valves) on MPC decision-making to ensure operational safety while achieving desired economic performance. In addition, even the tuning of classical control systems like proportional-integral-derivative control systems should account for the on/off state of safety systems as it impacts significantly the overall process dynamics.

Motivated by the above considerations, in the present work, we investigate how the activation of the safety system should be accounted for in the context of feedback controller design and implementation because the actions of the safety system change the process dynamics, and thus, they should be accounted for in the calculation of the feedback controller actions. Specifically, we focus on two industrially-important (from a safety point of view) case studies, a chemical reactor and a flash drum, and analyze the interaction of the control and safety systems both in the case where a model predictive control (MPC) design is employed (chemical reactor example) and in the case where a proportional-integral (PI) control design (flash drum example) is used. The paper is structured as follows: to demonstrate for the first time the integration of MPC with safety system activation, we first focus on the methyl isocyanate (MIC) hydrolysis reaction in a CSTR subject to disturbances that lead to reactor thermal runaway and demonstrate how the safety and control systems can work together to avoid thermal runaway. Secondly, we focus on valve malfunction for a flash drum to demonstrate that modifying the tuning parameters of a PI controller based on the safety system being on or off leads to improved closed-loop performance compared to the case in which the tuning parameters of the PI controller remain the same regardless of the state of the safety system.

2. Integration of safety and control systems: MIC reaction in a CSTR case study

The first case study is the methyl isocyanate (MIC) hydrolysis reaction in a CSTR (Ball, 2011), where MIC is the principal chemical involved in the Bhopal disaster. In this case study, we will seek to coordinate an MPC formulation (for this example, a specific MPC formulation known as Lyapunov-based MPC (LMPC) (Mhaskar et al., 2006) will be utilized to control the process) with the safety system. This section describes the MIC hydrolysis process. Section 3 describes the LMPC utilized to control the process, and the results obtained under disturbances without the safety system activated. Section 4 completes the discussion by developing a safety system for this example and a methodology for its interaction with the LMPC to enhance process operational safety.

The exothermic hydrolysis reaction of methyl isocyanate to the corresponding amine and carbon dioxide is given as follows:

$$CH_3NCO_{(l)} + H_2O_{(l)} \longrightarrow CH_3NH_{2(aq)} + CO_{2(aq)}$$

By applying mass and energy balances, the dynamic model of the process can be described as follows:

$$\begin{aligned} m\frac{dC_A}{dt} &= -mk_0 e^{\frac{-Ea}{RT}} C_A + F(C_{A0} - C_A) \\ mC_P\frac{dT}{dt} &= (-\Delta H)mk_0 e^{\frac{-Ea}{RT}} C_A + FC_P(T_0 - T) - L(T - T_j) \end{aligned} \quad (1)$$

where C_A is the concentration of MIC in the reactor in units of mol/kg, m is the total mass of the mixture in the reactor, and T is the temperature of the reactor. The concentration of reactant MIC in the feed and the feed temperature are denoted by C_{A0} and T_0, respectively. The flow rates of both the CSTR feed and outlet streams are denoted by F. The reacting liquid has a constant heat capacity of C_P. k_0, E_a and ΔH are the reaction pre-exponential factor, activation energy and the enthalpy of the reaction, respectively. The CSTR is equipped with a cooling jacket, for which the heat transfer coefficient is denoted by L, and the temperature of the cooling jacket is denoted by T_j. The reactor is simulated at the conditions reported for the Bhopal

Table 1 – Parameter values for the MIC reaction case study in a CSTR.

$T_0 = 293$ K	$F = 57.5$ kg/s
$m = 4.1 \times 10^4$ kg	$E_a = 6.54 \times 10^4$ J/mol
$k_0 = 4.13 \times 10^8$/s	$\Delta H = -8.04 \times 10^4$ J/mol
$C_P = 3000$ J/(kg K)	$R = 8.314$ J/(mol K)
$L = 7.1 \times 10^6$ J/(s K)	$C_{A_0} = 29.35$ mol/kg
$T_{j_s} = 293$ K	$C_{A_s} = 10.1767$ mol/kg
$T_s = 305.1881$ K	

catastrophe (Toro et al., 2016). Process parameter values are listed in Table 1. It is noted that the simulations of this process will assume that liquid in the CSTR can vaporize; we will continue to utilize Eq. (1) even when vaporization of liquid occurs because this allows key aspects of our proposed method for integrating the safety system and MPC to be explored despite the modeling approximation.

3. LMPC design and thermal runaway

3.1. LMPC design

The CSTR is initially operated at the steady-state MIC concentration and temperature of $[C_{A_s} T_s] = [10.1767$ mol/kg 305.1881 K], with steady-state jacket temperature $T_{j_s} = 293$ K. The control objective is to stabilize the states of the reactor at their steady-state values by adjusting the manipulated input (the cooling jacket temperature T_j) subject to the bounds $280\text{ K} \leq T_j \leq 300\text{ K}$. The states and the input of the closed-loop process will be represented in deviation variable form from this steady-state as $x^T := [C_A - C_{A_s}\ T - T_s]$ and $u := T_j - T_{j_s}$, so that it is desired to drive x and u to the origin. In this notation, the system of Eq. (1) can be written in the form of $\dot{x} = f(x) + g(x)u$, where $f(x)$ and $g(x)$ are nonlinear vector functions of the process state vector. We first design an LMPC to control the process. LMPC is an MPC formulation that utilizes stability constraints based on a Lyapunov function $V(\cdot)$ and an explicit stabilizing (Lyapunov-based) controller for the nonlinear process (denoted by $h(\cdot)$) to guarantee feasibility of the MPC and closed-loop stability of a nonlinear process operated under the MPC (in the sense that the closed-loop state is driven to a neighborhood of the origin under LMPC for all initial conditions in an explicitly characterizable region of state-space termed the stability region around the steady-state) when the disturbances and MPC sampling period are sufficiently small. Specifically, the LMPC scheme is formulated as the following optimization problem:

$$\min_{u \in S(\Delta)} \int_{t_k}^{t_{k+N}} (\|\tilde{x}(\tau)\|^2_{Q_c} + \|u(\tau)\|^2_{R_c})\, d\tau \tag{2a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}(t) = f(\tilde{x}(t)) + g(\tilde{x}(t))u(t) \tag{2b}$$

$$\tilde{x}(t_k) = x(t_k) \tag{2c}$$

$$u(t) \in U, \quad \forall t \in [t_k, t_{k+N}) \tag{2d}$$

$$\frac{\partial V(x(t_k))}{\partial x}(f(x(t_k)) + g(x(t_k))u(t_k)) \leq \frac{\partial V(x(t_k))}{\partial x}(f(x(t_k)) + g(x(t_k))h(x(t_k))) \tag{2e}$$

where $S(\Delta)$ is the set of piecewise constant functions with period Δ, and N is the number of sampling periods in the prediction horizon. The notation $t_k = k\Delta$, $k = 0, 1, \ldots$, denotes a sampling time of the LMPC at which the optimization problem of Eq. (2) is solved. The optimal input trajectory of the LMPC optimization problem, computed at t_k, is denoted by $u^*(t|t_k)$, which is calculated over the entire prediction horizon $t \in [t_k, t_{k+N})$. The control action computed for the first sampling period in the prediction horizon (i.e., $u^*(t_k|t_k)$) is applied at t_k for a sampling period, and the LMPC problem is re-solved at the next sampling time. The objective function to be minimized (Eq. (2a)) is the integral of $\|\tilde{x}(\tau)\|^2_{Q_c} + \|u(\tau)\|^2_{R_c}$ over the prediction horizon, where $||\cdot||_{Q_c}$ and $||\cdot||_{R_c}$ represent weighted Euclidean norms (weighted by matrices Q_c and R_c, respectively) utilized to penalize the deviations of the process states and manipulated inputs from their corresponding steady-state values in the objective function. The constraint of Eq. (2b) is the deviation form of Eq. (1) that is used to predict the states of the closed-loop system ($\tilde{x}$ represents the predicted process state that the LMPC computes based on this process model). Eq. (2c) defines the initial condition $\tilde{x}(t_k)$ of the optimization problem which is the state measurement $x(t_k)$ at time t_k. Eq. (2d) defines the input constraints applied over the entire prediction horizon. The constraint of Eq. (2e) decreases the value of the Lyapunov function $V(x)$ such that $x(t)$ moves toward the origin at least at the worst-case rate achieved by the Lyapunov-based controller $h(x)$, the form of which will be defined below. The explicit Euler method with an integration time step of $h_c = 10^{-2}$ s was applied to numerically simulate the dynamic model of Eq. (1) under the LMPC. The nonlinear optimization problem of the LMPC of Eq. (2) was solved using the IPOPT software package (Wächter and Biegler, 2006) with the following parameters: sampling period $\Delta = 1$ s; prediction horizon $N = 10$. $Q_c = [3\,0;05]$ and $R_c = 1$ are chosen such that the term related to the states and the term related to the input are on the same order of magnitude in $\|\tilde{x}(\tau)\|^2_{Q_c} + \|u(\tau)\|^2_{R_c}$.

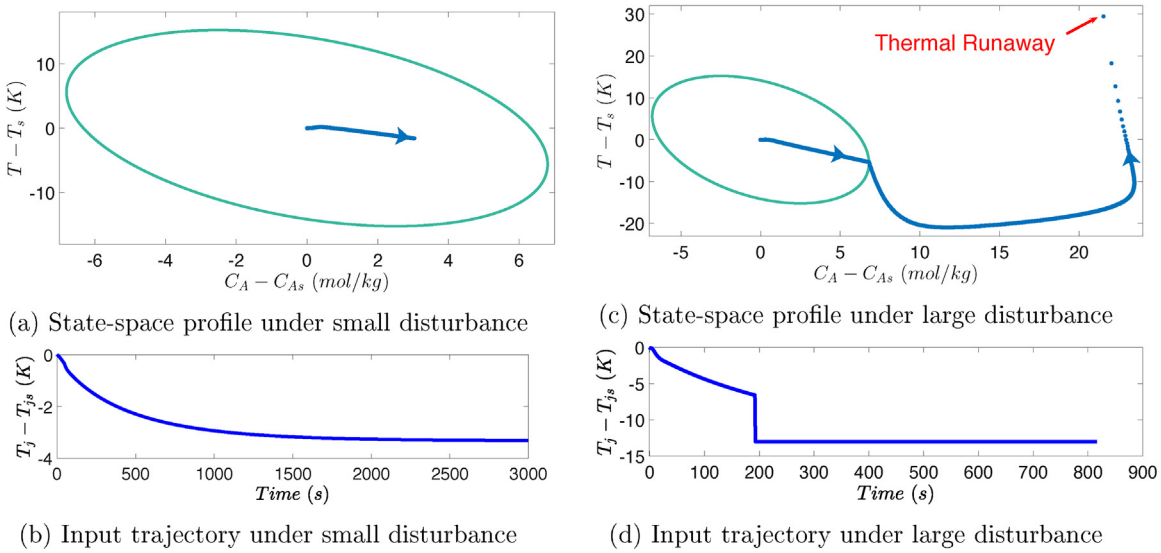
The Lyapunov function is designed using the standard quadratic form $V(x) = x^T P x$, where the positive definite matrix P is as follows: [200 33;33 40]. The stability region Ω_ρ is characterized as a level set of the Lyapunov function: $\Omega_\rho := \{x \in R^2 \mid V(x) \leqslant \rho\}$. For the system of Eq. (1), the stability region Ω_ρ with $\rho = 8000$ was chosen. This determination was made utilizing closed-loop simulations of the nonlinear process under the above Lyapunov function V and a Lyapunov-based controller to find a region within which the closed-loop state could be driven toward the origin under the controller $h(x)$ because the time derivative of the Lyapunov function was negative under this controller along the closed-loop state trajectories. The controller $h(x)$ was formulated as follows (Lin and Sontag, 1991):

$$h(x) = \begin{cases} -\dfrac{L_f V + \sqrt{L_f V^2 + L_g V^4}}{L_g V^2} L_g V & \text{if } L_g V \neq 0 \\ 0 & \text{if } L_g V = 0 \end{cases} \tag{3}$$

where $L_f V$ signifies the Lie derivative of V along the vector field f, and $L_g V$ is the Lie derivative of V along the vector field g.

3.2. Simulation results

A small feed disturbance (i.e., change of feed concentration from 29.35 mol/kg to 35 mol/kg) is initially considered and Fig. 1a and b demonstrate that the closed-loop system under the LMPC is robust to the small disturbance by stabilizing the system state at another steady-state within the stability region.



(a) State-space profile under small disturbance

(b) Input trajectory under small disturbance

(c) State-space profile under large disturbance

(d) Input trajectory under large disturbance

Fig. 1 – (a) and (b) demonstrate that the LMPC can stabilize the closed-loop state at another steady-state when there is a small disturbance. (c) and (d) demonstrate that the LMPC fails to keep the closed-loop state inside the stability region when there is a large disturbance. In (a,b) and (c,d), the respective disturbances are applied from the beginning of the time of operation. The large drop in T_j in (d) is forced at approximately 200 s when the closed-loop state exits the stability region (c). The point labeled "thermal runaway" in (c) corresponds to t = 800 s in (d). It is notable that though the same time interval is utilized between all points plotted in (c), separation is only visible between the data points toward the end of the simulation as thermal runaway is approached because it is at those times that the changes in temperature become rapid between the plotting intervals.

However, when there exists a large disturbance (i.e., the change of feed concentration is from 29.35 mol/kg to 70 mol/kg) due to, for example, failure of the device which distributes the feed, it is shown in Fig. 1c that the state exits the stability region and the manipulated input hits its lower bound to cool down the reactor as much as possible. However, after 800 s of implementation of maximum cooling, the reactor temperature starts to increase significantly. The reason for this increasing value of the temperature is that when the reactor temperature rises, the exothermic reaction rate also increases, causing a further increase in temperature, which is a dangerous phenomenon called thermal runaway. Therefore, it can be concluded that in the presence of large disturbances, the reactor may operate in an unsafe region due to the restriction of the control actuator, which motivates the development of a safety system to maintain reactor safety.

4. Integration of MPC with safety system

In this section, the safety system for the MIC hydrolysis process is first designed using two different safety mechanisms: (a) a safety relief valve; (b) cold water injection. Then, the entire process control/safety system which integrates the safety system with the LMPC is developed to maintain closed-loop safety and stability. Finally, the MIC reaction example is used to demonstrate the application of the proposed control/safety scheme.

4.1. *Components of safety system*

4.1.1. *Safety relief valve*

In the MIC hydrolysis example, we will consider the use of a valve in the reactor for which the opening is triggered by logic in the safety system (i.e., not by the process controller logic) to aid in preventing thermal runaway. The purpose of the valve in this example is to reduce the temperature of the reactor by discharging material when the temperature is high in the reactor (because the valve has this purpose and is part of the safety system, the valve in this example will be called a safety relief valve; however, it should be understood that it is not a pressure-actuated type of safety relief valve (Marlin, 2012)). In industry, thermal runaway may occur due to different failures, such as mischarging reactant or failures in the cooling system that affect the coolant temperature or flow rate. Since the above unsafe operating conditions are unpredictable and uncontrollable and thermal runaway can vaporize liquid in a reactor, a suitable and correctly sized relief system is crucially important as a backup method to prevent fatal accidents (Hace, 2013). The size of a relief valve is carefully chosen in practice. Specifically, if a relief valve is under-sized, high pressure and equipment failure may occur; if a relief device is over-sized, the relief system may become unstable during the operation and too much material may be wasted (Crowl and Tipler, 2013).

4.1.2. *Cold water injection*

Direct cold solvent injection can cool down a reaction mixture's temperature. For example, Vernières-Hassimi and Leveneur (2015) demonstrated in both simulation and experiment that cold water injection could rapidly lower the temperature in a reactor where an exothermic reaction took place. Cool water injection is utilized to prevent thermal runaway in the MIC hydrolysis example.

4.1.3. *Safety system for simulation*

In our simulation, high temperature is the trigger of the opening of the relief valve. Specifically, the valve opens once the temperature is higher than 320 K. To simplify the development, we assume that all the relief discharge flow is in liquid phase. The relief valve size is 4×10^{-3} m^2 (selected based on closed-loop simulations indicating that this size allowed the closed-loop state to re-enter the stability region when the

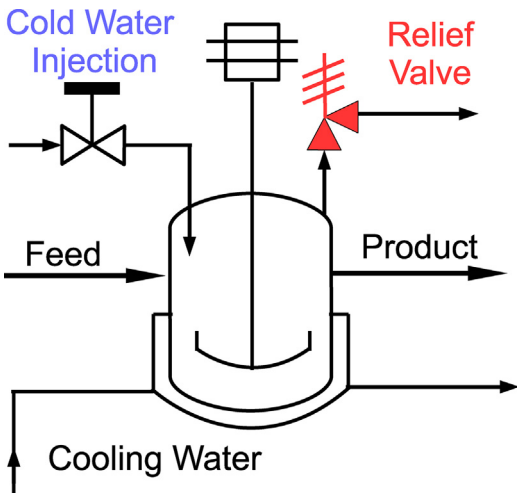


Fig. 2 – An example of CSTR with safety system for MIC hydrolysis, where the temperature of the cooling jacket is controlled by the LMPC.

safety system is activated in the simulations performed) and the relief flow is determined by the equation in Hace (2013):

$$G_{relief} = 0.9 \times 144 \times \frac{dP}{dt} \times \left(\frac{32.2}{778.16} \times \frac{T}{C_P} \right) \quad (4)$$

where G_{relief} is the mass of the mixture per area for flow through the relief valve (in kg/m^2), T is the temperature of the relief flow (K), C_p is the heat capacity in J/kg K, and the pressure P in the reactor (in Pa) is obtained from the Antoine equation, with parameters of this equation estimated from data in the process simulation software Aspen Plus.

Cool water is injected with a temperature of 280 K if the temperature in the reactor exceeds 320 K, and the mass flow rate of this injected cold water is the same as the mass flow rate of material leaving through the relief valve; thus, the total mass in the reactor remains unchanged when the safety system is activated. Fig. 2 depicts the CSTR under consideration, with the cooling water system that is manipulated using the LMPC depicted, as well as the two elements of the safety system.

4.2. *Logic integrating control and safety systems*

A methodology for integrating the LMPC with the activation of the safety system is developed to avoid thermal runaway when the LMPC fails to maintain the closed-loop state inside the stability region in the presence of large disturbances. This methodology is based on dividing the state-space into three different regions which correspond to various combinations of control and safety system actions. A schematic of these different regions and an example closed-loop state trajectory are shown in Fig. 3. The different combinations of control and safety system actions in the three regions are as follows:

Region 1 (stability region): When the closed-loop state is inside the stability region, the LMPC is implemented to maintain the closed-loop state in a neighborhood of the origin even if there continuously exist small disturbances. In this region, the safety system is not activated.
Region 2 (unsafe operating region): If large disturbances are introduced to the reactor, the state may come out of the stability region. In order to enhance process operational safety, the manipulated input (i.e., T_j) is set to its lower bound, namely the lowest cooling jacket temperature, since the LMPC may not drive the closed-loop state back into the stability region once the state exits the stability region.
Region 3 (thermal runaway region): If large disturbances keep affecting the reactor and the maximum cooling is not able to lower the temperature sufficiently, then the reactor temperature may reach a high value (i.e., the lower boundary of Region 3). The safety system takes action in Region 3. Specifically, the relief valve opens immediately after the state enters Region 3 and stays open until the state goes back to Region 1. Meanwhile, cold water is injected into the reactor, cooling down the reactor. Injection stops once the relief valve is closed (state goes back into Region 1). At the same time, the jacket temperature stays at its lower bound to apply maximum cooling.

Region 1 is the stability region of the closed-loop system under LMPC defined by $\Omega_\rho = \{x \in R^2 \mid V(x) \leq \rho\}$. The Region 2 and Region 3 were separated by a boundary obtained by finding the highest feasible temperature, which is the trigger of the relief valve. This temperature need not to be very high since the temperature increases very fast once it reaches a certain temperature, which is around 320 K, and this is why we took this temperature to be 320 K in the safety system logic.

The implementation of the logic integrating safety and control systems could be done by a supervisory system that specifies the actions of the control and safety system according to the specified logic.

4.3. *Simulation results*

In Fig. 4, it is demonstrated that in the presence of a large disturbance, the LMPC integrated with the safety system via the above logic succeeds at avoiding thermal runaway and drives the state back to the origin. At the beginning of the simulation, a large disturbance (i.e., the feed concentration is changed from 29.35 mol/kg to 70 mol/kg as in Section 3.2) is introduced into the reactor, resulting in the failure of the LMPC to keep the system state within the stability region. After about 600 s, since the heat generated by the reaction is much more than the heat that the cooling system can remove, the concentration of the reactant increases to such an extent that the temperature starts to increase rapidly and reaches the safety limit of 320 K. Once the temperature exceeds the safety limit, the relief valve opens to discharge hot fluid from the reactor and an additional stream is employed to feed fresh water into the reactor. The liquid relief flow rapidly decreases the total internal energy and the reactant concentration in the reactor. Cool water promptly lowers the reactor temperature and dilutes the reactant, lowering its concentration. The safety system is activated for about 10 s to drive the closed-loop state back into Region 1. Once the closed-loop state goes back to Region 1, the safety system is shut off and the LMPC is utilized instead to stabilize the system state at the origin. Inside Region 1, the LMPC is guaranteed to drive the closed-loop state toward the origin when there are no disturbances and when the sampling period is sufficiently small (Mhaskar et al., 2006; Albalawi et al., 2018). It should be noted that if the large disturbance still exists after the closed-loop system state goes back into Region 1, then the logic of Section 4.2 will again be implemented to avoid thermal runaway as discussed above. Because it is not desirable to have the safety system activated regularly, this indicates that some diagnostics may need to be performed after the safety system is shut off to analyze the

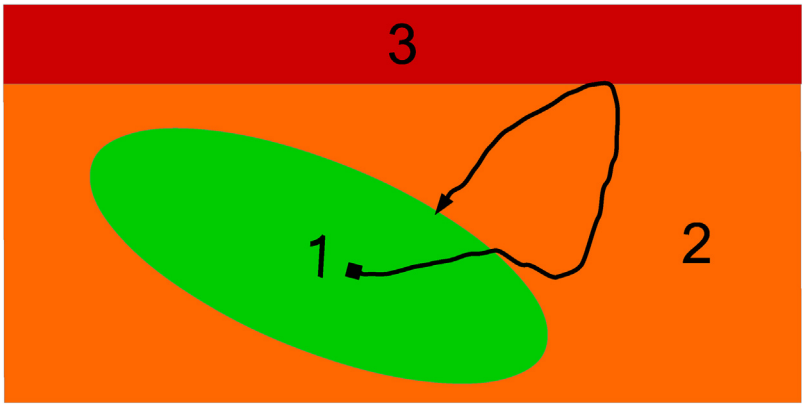


Fig. 3 – A schematic showing, in the $C_A - T$ state-space (with T considered to be on the y-axis and C_A considered to be on the x-axis), the stability region (green), unsafe operating region (orange), and the thermal runaway region (red), together with an example trajectory starting from the origin. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of the article.)

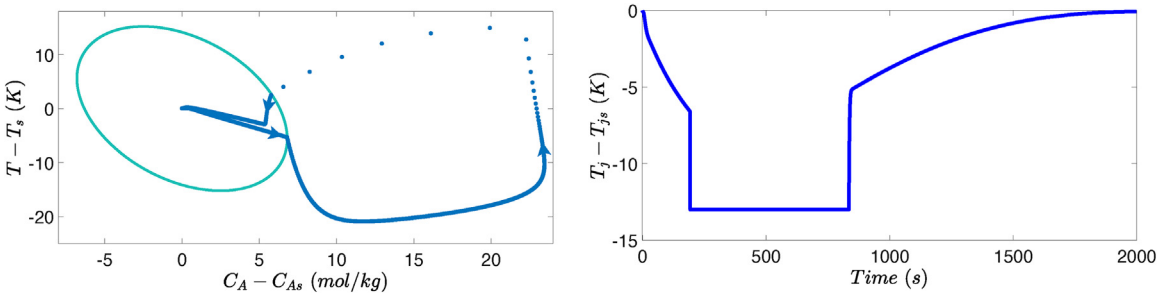


Fig. 4 – State-space plot and input plot of LMPC integrated with the safety system for the MIC hydrolysis reaction in a CSTR. The drop in the coolant temperature when the state exits the stability region is noticeable until the state re-enters the stability region and the LMPC begins to be used once again to manipulate T_j and drive the process state toward its steady-state value. The time interval is the same between the plotting of each data point in the state-space plot. Therefore, the large differences in the state between plotted points as the system approaches thermal runaway indicate rapid changes in temperature. The large differences in the state between plotted points as the state is driven back toward the stability region after the safety system is activated indicate the effectiveness of the safety system's actions to rapidly move the state back toward the stability region.

process and determine how to prevent further activations of the safety system.

Remark 1. We note that PI control can be used to regulate the CSTR at the steady-state; however, it is not possible to account for the impact of control actuator constraints directly in the controller design and calculate stability regions in an explicit manner, and thus, determine a safety logic to integrate the control and safety systems as is done in the case of MPC.

Remark 2. Several points should be made regarding the MIC hydrolysis example. First, it should be noted that no attempt was made to analyze all possible combinations of control and safety system actions, encompassing all initial conditions or all possible disturbances, to ensure that the policy developed would drive the closed-loop state back to the stability region under any conditions. Rather, the example was meant to demonstrate that through careful coordination of the control and safety systems, which here was undertaken for the conditions simulated, it is possible to enhance operational safety beyond what might be achieved utilizing the control system alone. Another goal of the example was to demonstrate that the integration of the control and safety systems may aid in keeping the process on-line for economic reasons, despite the safety issues, by allowing the safety system actions to be designed such that they drive the closed-loop state back into the stability region where the controller can be utilized to regulate the process state to the steady-state. In an industrial setting, a more in-depth analysis of all potential hazardous situations should be undertaken to ensure that the control and safety system combination handles all of these and achieves the desired behavior in each case (e.g., that there are no cases where the control and safety system actions may cool the reactor but not drive the closed-loop state back into the stability region, so that the cooling does not stop under the pre-determined interaction policy for the control and safety systems). In addition, consideration would need to be given to what should happen if the safety systems are triggered, even if the closed-loop state does re-enter the stability region (for example, does any type of shut-down or correction procedure need to follow). Additionally, it should be noted that the concept of coordinating an MPC and the safety systems is not limited to LMPC. LMPC has the nice property for such coordination that an explicitly characterizable (*a priori*) region exists from which the closed-loop state can be guaranteed to be maintained in the presence of sufficiently small disturbances and a sufficiently small sampling period. This aided in the development of Region 1 in this example. However, in general, any MPC design could be utilized in conjunction with a safety system with sufficient care taken to identify all potential combinations of safety and control system actions required. Third, care must be taken in disposing of any chemicals that exit

through the relief valves to ensure that toxic species do not enter the environment; however, detailed consideration of this point is outside the scope of this work.

5. Integration of safety and control systems: flash drum case study

In the next several sections, we develop a second case study in which we focus on a high-pressure flash drum used to separate a typical mixture in the chemical industry. The liquid level and the temperature in the flash drum can be regulated by two PI controllers, and this control system is integrated with a pressure relief valve. In this study, we demonstrate that in a scenario in which the valve regulating the outlet vapor stream from the drum experiences a fault that leads to a significant pressure rise inside the flash drum, modifying the tuning parameters of one of the other PI controllers when the safety system is activated leads to improved closed-loop performance compared to the case in which the tuning parameters of that PI controller remain the same regardless of the state of the safety system. Specifically, the next section describes the flash drum process under consideration, and Section 7 describes the tuning/re-tuning method utilized for the PI controller for which the tuning changes when the safety system is activated and demonstrates the benefits of this controller updating through closed-loop simulations.

6. Flash drum process description and relief valve design

A flash process (Marlin, 1995), as shown in Fig. 5, is used to separate a mixture of methane (10%), ethane (20%), propane (30%), butane (35%) and pentane (5%) to a separation level that makes the bottom and top flash outlet streams suitable feeds for downstream distillation towers. Specifically, a liquid feed stream of flow rate F, mole fraction z_i of component i, temperature T_f and pressure P_f is initially heated by a heat exchanger with heating duty Q to a temperature T_{in} and corresponding pressure P_{in}. This heated stream passes through a throttling valve and is then separated adiabatically in the flash drum into a liquid stream of flow rate L with composition x_i and a vapor stream of flow rate V with composition y_i. Both the liquid and vapor streams exiting the flash drum have temperature T and pressure P. The five components are separated due to different vapor pressures. The feed temperature T_f is 40 °C, the feed pressure P_f is 45 bar, the drum height is 4 ft and the drum diameter is 1 ft. The mole fractions of ethane, i-butane, methane, n-butane, n-pentane, and propane in the feed stream (i.e., the z_i) are 0.2, 0.15, 0.1, 0.2, 0.05, and 0.3, respectively.

To model a flash drum process, we need to apply component molar balances, an energy balance, and phase equilibrium relationships to the process to end up with a nonlinear dynamic system (i.e., systems of first-order nonlinear ordinary differential equations) with the following state variables: drum pressure P, drum temperature T, number of moles N_i of component i in the drum, mole fractions y_i and x_i of component i the in vapor and liquid phases, and the total number of moles N^V and N^L in the vapor phase and liquid phase, respectively. This model was developed within the Aspen Plus Dynamics software environment and was used to dynamically simulate the flash drum. In Aspen Plus Dynamics, the process model follows the schematic shown in Fig. 5. The detailed model equations are omitted for brevity but the model is readily available from the authors.

The flash drum example, which is a process modeled by a large number of nonlinear ordinary differential equations, demonstrates that the proposed approach can be applied to larger systems and is not limited only to those with very few states.

Two control loops are shown in Fig. 5 which are regulated by PI controllers. Specifically, PI controllers are utilized as the level controller (LC) that adjusts the liquid effluent valve to maintain the liquid level in the drum at a desired value, and as the temperature controller (TC) that adjusts the feed temperature to maintain the drum temperature T at a desired set-point value using the heating duty Q as the manipulated input. Since the drum temperature and the drum pressure are related through thermodynamics, controlling the drum temperature indirectly allows manipulation of the drum pressure P.

Under normal operation, during which process equipment such as pressure sensors and valves operate properly, the two controllers can maintain the level and temperature (and indirectly the pressure) near the desired values (Marlin, 1995). However, a variety of fault conditions may cause an unsafe situation to occur in which an extremely high pressure may be reached in the drum (potential causes of such unsafe conditions may be faults in the top vapor effluent valve and the bottom liquid effluent valve that cause them to close). Therefore, a pressure relief valve is designed to prevent a potentially dangerous high-pressure situation by allowing pressure relief in the flash drum even if faults occur in the vapor and liquid effluent valves.

The pressure relief valve considered in this example is a safety device designed to protect a pressurized vessel during an overpressure event and is pressure-actuated by physical means (in contrast to the type of valve termed a “safety valve” in the MIC hydrolysis example, which was actuated through electrical signals based on temperature). The pressure relief valve for the flash drum in this example was designed using Aspen Plus. Since a potentially dangerous failure situation occurs when the vapor effluent valve fails, we determine the pressure relief valve parameters based on the case in which the vapor valve is totally closed. The required mass flow rate through the relief valve to quickly lower the drum pressure in such an event is calculated as the minimum mass flow rate required to keep the pressure in the drum below the maximum pressure which it can sustain; this mass flow rate is 523 kg/h as calculated by Aspen Plus. Considering relieving conditions, fluid properties and operating conditions, a standardized orifice size of 8.303 cm^2 is used to meet the required relief flow rate.

Since the flash drum operating pressure is 10 bar and the highest allowable drum pressure is considered to be 12 bar, the opening (set) pressure of the pressure relief valve is chosen as 10.5 bar. The resetting pressure (at which the pressure relief valve closes) is set at 9 bar so that the relief valve will not close once it opens until the process equipment failure that caused the high-pressure situation is fixed. The discharge flow is considered to be only vapor. The flash calculation is based on constant enthalpy. The relief flow is considered to be a compressible fluid and the discharge coefficient is 0.96.

Remark 3. The open-loop steady state of the flash drum process is an asymptotically stable one and the same is true for the closed-loop system steady-states under different relief

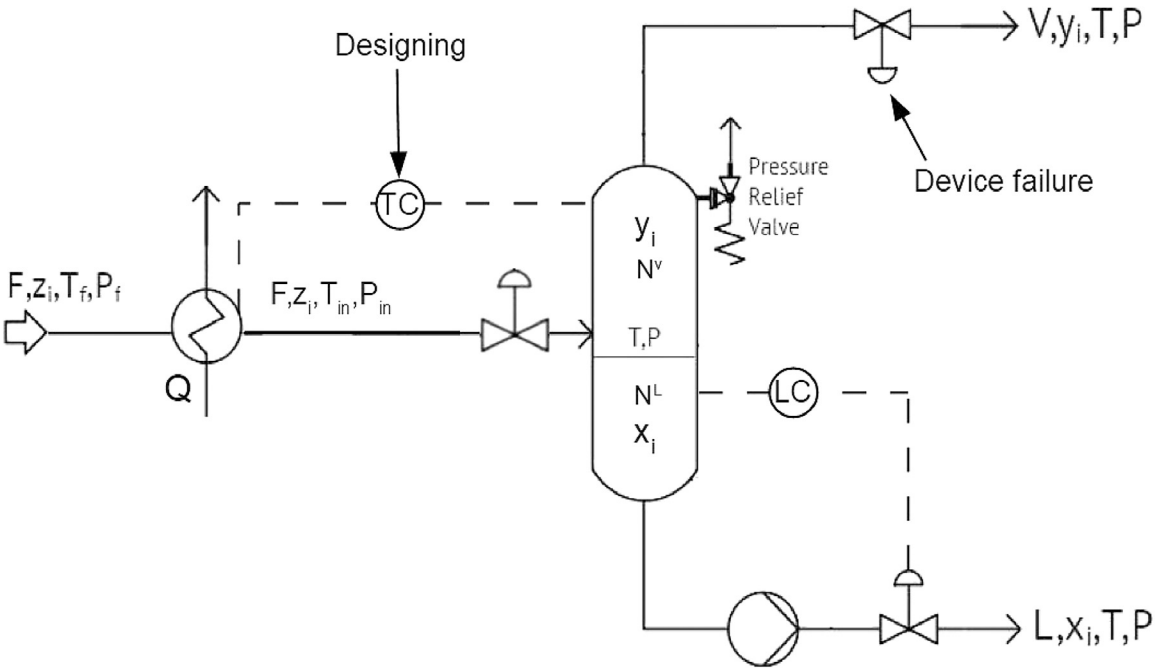


Fig. 5 – A schematic of the flash process. The temperature controller for which the tuning is changed to account for safety system activation is pointed out in the figure with the word "Designing." The vapor effluent valve experiencing the failure is pointed out in the figure with "Device failure." The three units shown in the figure besides the valves and controllers are, from left to right, a heat exchanger, flash drum, and pump.

valve settings. This conclusion was obtained by running open-loop and closed-loop simulations as the use of a large-scale simulator used to simulate the flash drum process does not allow the analytic evaluation of the eigenvalues of the Jacobian linearization of the open-loop and closed-loop process around the steady-states. With respect to the use of two PI controllers and the interaction between the loops, we carried out closed-loop simulation runs in which a set-point change is requested in one output and the other output is requested to stay at its steady-state value and we found minimal interaction between the two control loops, thereby justifying the use of single-loop PI control.

7. Feedback controller design

7.1. Control objective and device failure

The flash drum is initially operated at the desired operating steady-state. After the drum operates at this steady-state for 0.002 h, the vapor effluent valve closes from 50% open to 0% open (i.e., it becomes fully closed) as the result of a fault. As a result of this failure, the pressure in the drum rises rapidly, reaching the opening pressure of the pressure relief valve. The pressure relief valve then opens to discharge high-pressure vapor. Both the drum temperature and drum pressure then drop. Since the pressure relief valve changes the system dynamics and PI controllers are tuned with respect to the process dynamics, more effective control of the flash drum process may be obtained during the time that the safety relief system is activated by changing the tuning of a PI controller when the pressure relief valve is open than by leaving the tuning unchanged. In the rest of this section, we explore this by developing two sets of PI control parameters for the temperature controller for the flash drum process: one which is utilized when the pressure relief valve is closed, and one which is utilized when it is open. The control objective is to maintain the drum temperature at the set-point in the presence of the failure of the vapor effluent valve, and to operate the flash drum safely before, during and after the pressure relief valve is opened (where safe operation for this example corresponds to the drum pressure remaining less than the flash drum maximum operating pressure of 12 bar at all times). To allow the impact of re-tuning a controller to account for safety system activation to be clearly analyzed, the tuning of the level controller ($K_c = 10$ and $\tau_I = 3600$ s) is not adjusted when the tuning for the temperature controller is adjusted (i.e., the tuning for the level controller remains at the same value throughout the time of operation).

7.2. PI controller tuning

To develop the two sets of PI tuning parameters for the temperature controller for the cases that the relief valve is closed and when it is open, we first develop empirical linear models between the drum temperature and feed heating duty for both cases to determine the PI controller tuning parameters. Using the transient response of the drum temperature subject to a step change in the feed heating duty from its initial steady-state value, a first-order transfer function model is determined to describe the process dynamics. Specifically, data on the drum temperature T and feed heat duty Q is collected from open-loop simulations in Aspen Plus Dynamics software for a variety of step changes in Q. Then, the maximum likelihood estimation (MLE) method is applied in MATLAB to this data to identify the parameters in the following single-input–single-output model:

$$y(s) = \frac{b}{s+a}u(s) \tag{5}$$

where y is the drum temperature (in deviation form from its steady-state value) in C and u is the heat duty (in deviation form from its steady-state value) in kW. The differences

Table 2 – Parameter values of the linear empirical model of Eq. (5) when the relief valve is closed and before any fault occurs in the pressure control loop to cause the vapor effluent valve to close (denoted by "no fault or relief valve" in the table) and after the vapor effluent valve closes and the relief valve is opened (denoted by "with fault and relief valve" in the table).

No fault or relief valve	With fault and relief valve
$b = 0.0202$ $a = 0.105$	$b = 0.0206$ $a = 0.113$

Table 3 – Parameter values PI controller for the flash drum inlet temperature when the relief valve is closed and before any fault occurs in the pressure control loop to cause the vapor effluent valve to close (denoted by "no fault or relief valve" in the table) and after the vapor effluent valve closes and the relief valve is opened (denoted by "with fault and relief valve" in the table).

No fault or relief valve	With fault and relief valve
$K_c = 4$ $\tau_I = 14\,s$	$K_c = 6$ $\tau_I = 10\,s$

among the transfer functions obtained from the different step changes in Q are negligible. The model parameter values a and b for both cases are given in Table 2.

It needs to be mentioned that the system model identified when the relief valve is open is specific to the fault that occurred since this specific fault also impacts the dynamics of the flash drum. This means that the PI tuning parameters for the case with the fault and relief valve open are also specific to the fault that occurred because it is based on the model identified for that specific scenario. In our example, the system model with the relief valve open is identified when there is a device failure corresponding to the vapor effluent valve closed from 50% to 0% open. Attempts to integrate the safety and PI control systems for an industrial system would need to account for the variety of potential fault scenarios to develop a set of PI controller tunings effective for the different possible scenarios.

Based on the above two linear system models, a PI controller is applied using the following standard form:

$$\begin{aligned} e(t_k) &= T^{set} - T(t_k) \\ u_{PI}(t_k) &= K_c\left(e(t_k) + \frac{1}{\tau_I}\int_0^{t_k} e(\tau)\,d\tau\right) \\ Q(t_k + \Delta t) &= Q(t=0) + u_{PI}(t_k) \\ 0 \le\ & Q(t_k + \Delta t) \le Q_{max} \end{aligned} \tag{6}$$

where t_k and Δt are current time and sample time interval. The error $e(t_k)$ between the temperature set-point $T^{set} = 25\,^{\circ}C$ and temperature measurement $T(t_k)$ at time t_k is calculated every sample interval. $Q(t=0) = 87.2625\,kW$ is the heat duty at the initial steady-state and $Q(t_k + \Delta t)$ is the heat duty for the next sample interval. 0 and $Q_{max} = 160\,kW$ represent the lower and upper bounds on the heat duty, respectively. $u_{PI}(t_k)$ represents the control action computed by the temperature controller at time t_k. The controller gain K_c and the controller integral time τ_I used in Eq. (6) for the case that the relief valve is closed and the vapor effluent valve can open, and for the case that the relief valve is open and the vapor effluent valve is closed, are shown in Table 3. These were developed using the two different models of Eq. (5).

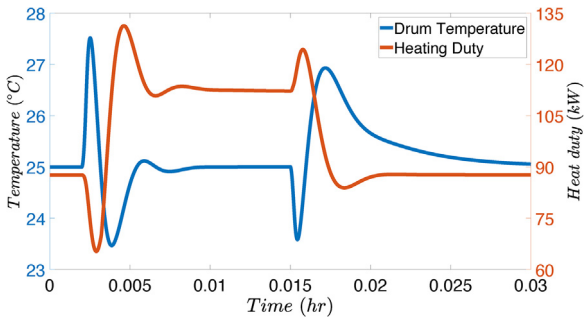


Fig. 6 – Controlled output and manipulated input for the temperature controller of the flash drum process with the tuning varying to account for the activation of the safety system.

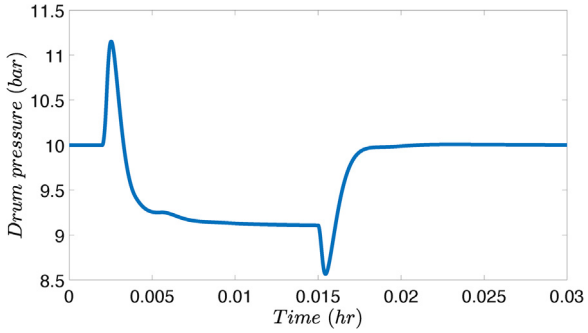


Fig. 7 – Drum pressure for the flash drum process with a varying tuning of the temperature controller to account for the activation of the safety system.

7.3. *Simulation results*

The flash drum process including the temperature controller with a tuning that is updated when the safety system activates is dynamically simulated in Aspen Plus Dynamics. Fig. 6 shows that after the vapor effluent valve is closed at $t = 0.002$ h, the drum temperature increases rapidly. The temperature controller reduces the heat duty such that the temperature difference between the current drum temperature and the set-point value will be decreased. However, it is observed in Fig. 7 that the dynamics of the temperature controller do not allow it to reduce the pressure in the drum rapidly enough to prevent the relief valve from opening, and the pressure relief valve opens when the drum pressure reaches its set pressure of 10.5 bar. As discussed above, different PI controller tuning parameters are utilized for the temperature controller before the vapor effluent valve closes and then after the opening of the relief valve. After the relief valve opens, the drum temperature and pressure decrease due to not only the pressure relief valve, but also the decreasing heating duty computed by the temperature controller. Eventually, after the pressure relief valve has been open for some time, the heating duty stabilizes to maintain the drum temperature at its normal operating temperature, which is the set-point temperature value used in the PI controller for the heating duty.

Around time $t = 0.015$ h, we assume that the fault resulting in closure of the vapor effluent valve is resolved and the vapor effluent valve returns to 50% opening. Due to the abrupt opening of the vapor valve, the drum pressure suddenly drops and reaches its resetting pressure of 9 bar. The pressure relief

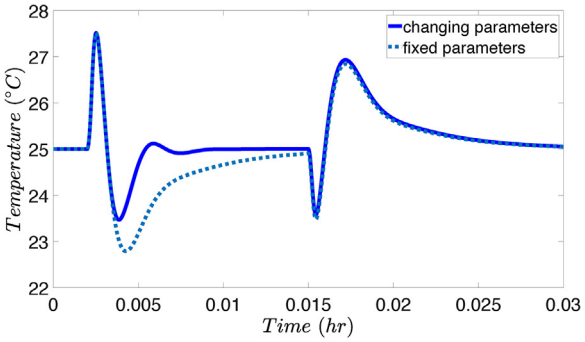


Fig. 8 – Temperature in the flash drum, with a varying tuning of the temperature controller ("changing parameters") to account for the activation of the safety system and with no change in the tuning of the temperature controller ("fixed parameters") when the safety system is activated.

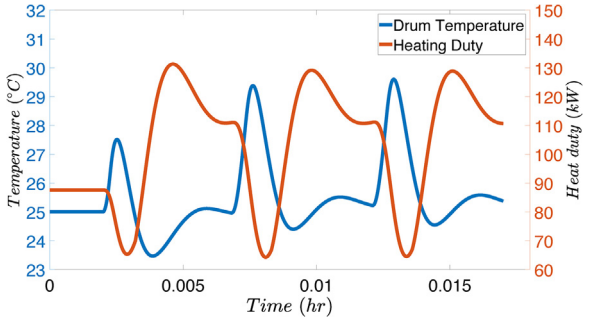


Fig. 9 – Drum temperature and heating duty for the flash drum process with a varying tuning of the temperature controller to account for the activation of the safety system when the resetting pressure of the relief valve is set at 9.2 bar.

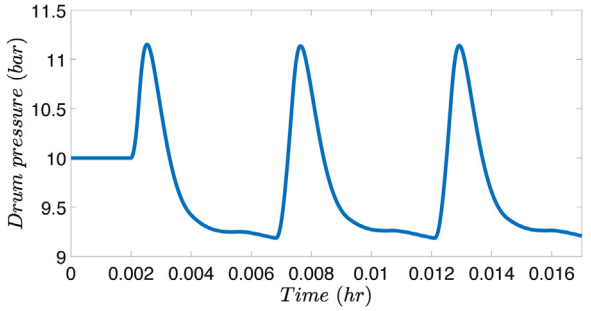


Fig. 10 – Drum pressure for the flash drum process with a varying tuning of the temperature controller to account for the activation of the safety system when the resetting pressure of the relief valve is set at 9.2 bar.

valve is closed once the drum pressure is below the resetting pressure and the parameters of the PI controller for the heat duty are changed back to their original values from before the relief valve opened. Shortly after 0.015 h, after the drum temperature and pressure drop, the drum temperature increases and overshoots its set-point value. Then, the controllers drive the drum temperature back to its set-point and the system is eventually again operated at its normal operating conditions.

Fig. 8 shows the temperature in the flash drum (i.e., the response of the closed-loop system) over time as the vapor effluent valve is opened and closed and the relief valve is activated when the tuning of the temperature controller is fixed throughout the time of operation and when the parameters vary according to Table 3 based on the state of the safety system. The figure demonstrates that after the relief valve opens, the temperature controller with an updated tuning to account for the safety system activation varies the drum temperature in a smaller range compared to the temperature controller with a fixed tuning regardless of the safety system state. This temperature controller with an updated tuning also returns the temperature in the flash drum to its set-point more rapidly than the controller with the fixed tuning, leading to improved closed-loop performance.

It is worth pointing out that the pressure relief valve resetting pressure must be sufficiently low so that the relief valve will not close before the fault resulting in the closing of the vapor effluent valve has been fixed. If the pressure relief valve closed when the vapor effluent valve is still closed, the relief valve would eventually open again because the drum pressure will increase due to closure of the vapor effluent valve, and consequently, an oscillation can occur in the closure of the relief valve, which is undesirable and also has the potential to be dangerous (e.g., if it wears the safety relief valve). To demonstrate this, a simulation where the resetting pressure is set at 9.2 bar (higher than the 9 bar utilized in Figs. 6–8) is shown in Figs. 9 and 10. In these figures, when the drum pressure drops to 9.2 bar, the relief valve is closed, and then the drum pressure increases rapidly until the relief valve opens again; this phenomenon should be avoided by using a lower resetting pressure for the safety relief valve. This indicates that to coordinate the control and safety systems effectively, it may be necessary to design these systems together (i.e., trying to determine an appropriate resetting pressure without analyzing the safety system's integration with the control system may result in too high of a resetting pressure being chosen so that the control and safety systems cannot be effectively coordinated). Furthermore, it indicates that closed-loop simulations may aid in determining an effective resetting pressure, since in general the pressure in a vessel may vary according to a nonlinear, coupled process dynamic model (where these dynamics change upon the activation of the safety system) under potentially different disturbances over time which are unknown *a priori*. It may also be helpful, when possible, to allow for manual relief valve opening and closure in the design of the valve to aid in handling issues with resetting pressure that could not be handled during the initial selection of the resetting pressure.

8. Conclusion

This work considered two case studies to analyze the interaction between control and safety systems. In the first case study, an LMPC system integrated with the activation of a safety system was developed for the MIC reaction in a CSTR to avoid thermal runaway. We first demonstrated that the closed-loop system state under the LMPC was maintained within the stability region in the presence of small disturbances. In the presence of large disturbances, it was demonstrated that an LMPC integrated with a safety system could maintain process safety in the sense of avoiding thermal runaway and driving the process state back into the stability region even after it exited it. In the second case study, we focused on a flash drum under PI control integrated with a pressure relief valve. In this study, we demonstrated that modifying the parameters of a PI controller based on the safety system being on or off can lead to improved closed-loop performance compared to the

case in which the parameters of the PI controller remain fixed regardless of the actions of the safety system.

Acknowledgments

Financial support from the National Science Foundation and the Department of Energy is gratefully acknowledged.

References

AIChE, 1994a. Dow's Chemical Exposure Index Guide, first ed. AIChE, New York, NY.

AIChE, 1994b. Dow's Fire and Explosion Index Hazard Classification Guide, seventh ed. AIChE, New York, NY.

Albalawi, F., Alanqar, A., Durand, H., Christofides, P.D., 2016. A feedback control framework for safe and economically-optimal operation of nonlinear processes. AIChE J. 62, 2391–2409.

Albalawi, F., Durand, H., Alanqar, A., Christofides, P.D., 2018. Achieving operational process safety via model predictive control. J. Loss Prev. Process Ind., http://dx.doi.org/10.1016/j.jlp.2016.11.021 (in press).

Albalawi, F., Durand, H., Christofides, P.D., 2017. Process operational safety using model predictive control based on a process Safeness Index. Comput. Chem. Eng. 104, 76–88.

Allen, J.T., El-Farra, N.H., 2017. A model-based framework for fault estimation and accommodation applied to distributed energy resources. Renew. Energy 100, 35–43.

Ball, R., 2011. Oscillatory thermal instability and the Bhopal disaster. Process Saf. Environ. Prot. 89, 317–322.

Bø, T.I., Johansen, T.A., 2014. Dynamic safety constraints by scenario based economic model predictive control. In: Proceedings of the IFAC World Congress, Cape Town, South Africa, pp. 9412–9418.

Center for Chemical Process Safety, 2008. Guidelines for Hazard Evaluation Procedures, third ed. John Wiley & Sons, Inc., Hoboken, NJ.

Christofides, P.D., Scattolini, R., Muñoz de la Peña, D., Liu, J., 2013. Distributed model predictive control: a tutorial review and future research directions. Comput. Chem. Eng. 51, 21–41.

Çinar, A., Palazoglu, A., Kayihan, F., 2007. Chemical Process Performance Evaluation. CRC Press, Boca Raton, FL.

Crowl, D.A., Tipler, S.A., 2013. Sizing pressure-relief devices. Chem. Eng. Prog., 68–76.

Ellis, M., Durand, H., Christofides, P.D., 2014. A tutorial review of economic model predictive control methods. J. Process Control 24, 1156–1178.

Ellis, M., Durand, H., Christofides, P.D., 2016. Elucidation of the role of constraints in economic model predictive control. Annu. Rev. Control 41, 208–217.

Ellis, M., Liu, J., Christofides, P.D., 2017. Economic Model Predictive Control: Theory, Formulations and Chemical Process Applications. Springer, Switzerland.

Gajjar, S., Palazoglu, A., 2016. A data-driven multidimensional visualization technique for process fault detection and diagnosis. Chemom. Intell. Lab. Syst. 154, 122–136.

Hace, I., 2013. The pressure relief system design for industrial reactors. J. Ind. Eng. 2013, 1–14.

Kettunen, M., Zhang, P., Jämsä-Jounela, S.L., 2008. An embedded fault detection, isolation and accommodation system in a model predictive controller for an industrial benchmark process. Comput. Chem. Eng. 32, 2966–2985.

Lao, L., Ellis, M., Christofides, P.D., 2013. Proactive fault-tolerant model predictive control. AIChE J. 59, 2810–2820.

Leveson, N.G., Stephanopoulos, G., 2014. A system-theoretic, control-inspired view and approach to process safety. AIChE J. 60, 2–14.

Lin, Y., Sontag, E., 1991. A universal formula for stabilization with bounded controls. Syst. Control Lett. 16, 393–397.

Mannan, M.S., Sachdeva, S., Chen, H., Reyes-Valdes, O., Liu, Y., Laboureur, D.M., 2015. Trends and challenges in process safety. AIChE J. 61, 3558–3569.

Marlin, T., 2012. Operability in Process Design: Achieving Safe, Profitable, and Robust Process Operations. McMaster University, Ontario, Canada.

Marlin, T.E., 1995. Process Control: Designing Process and Control Systems for Dynamic Performance. McGraw-Hill, New York.

Marsh & McLennan Companies Inc, 2016. The 100 Largest Losses 1974–2015: Large Property Damage Losses in the Hydrocarbon Industry. Technical Report.

Mayne, D.Q., Rawlings, J.B., Rao, C.V., Scokaert, P.O.M., 2000. Constrained model predictive control: stability and optimality. Automatica 36, 789–814.

Mhaskar, P., 2006. Robust model predictive control design for fault-tolerant control of process systems. Ind. Eng. Chem. Res. 45, 8565–8574.

Mhaskar, P., El-Farra, N.H., Christofides, P.D., 2006. Stabilization of nonlinear systems with state and control constraints using Lyapunov-based predictive control. Syst. Control Lett. 55, 650–659.

Mhaskar, P., Liu, J., Christofides, P.D., 2013. Fault-Tolerant Process Control: Methods and Applications. Springer-Verlag, London, England.

Morari, M., Lee, J.H., 1999. Model predictive control: past, present and future. Comput. Chem. Eng. 23, 667–682.

Prakash, J., Patwardhan, S.C., Narasimhan, S., 2002. A supervisory approach to fault-tolerant control of linear multivariable systems. Ind. Eng. Chem. Res. 41, 2270–2281.

Qin, S.J., Badgwell, T.A., 2003. A survey of industrial model predictive control technology. Control Eng. Pract. 11, 733–764.

Rawlings, J.B., 2000. Tutorial overview of model predictive control. IEEE Control Syst. Mag. 20, 38–52.

Smith, H., Howard, C., Foord, T., 2003. Alarms management/priority, floods, tears or gain? Introduction to the "problem". Meas. Control 36, 109–113.

Toro, J.C.O., Dobrosz-Gómez, I., García, M.Á.G., 2016. Dynamic modeling and bifurcation analysis for the methyl isocyanate hydrolysis reaction. J. Loss Prev. Process Ind. 39, 106–111.

Venkatasubramanian, V., 2011. Systemic failures: challenges and opportunities in risk management in complex systems. AIChE J. 57, 2–9.

Venkatasubramanian, V., Rengaswamy, R., Kavuri, S.N., 2003. A review of process fault detection and diagnosis: Part II: Qualitative models and search strategies. Comput. Chem. Eng. 27, 313–326.

Vernières-Hassimi, L., Leveneur, S., 2015. Alternative method to prevent thermal runaway in case of error on operating conditions continuous reactor. Process Saf. Environ. Prot. 98, 365–373.

Wächter, A., Biegler, L., 2006. On the implementation of an interior-point filter line-search algorithm for large-scale nonlinear programming. Math. Program. 106, 25–57.

Wang, J., Yang, F., Chen, T., Shah, S.L., 2016. An overview of industrial alarm systems: main causes for alarm overloading, research status, and open problems. IEEE Trans. Autom. Sci. Eng. 13, 1045–1061.

Xue, D., El-Farra, N.H., 2016. Actuator fault-tolerant control of networked distributed processes with event-triggered sensor-controller communication. In: Proceedings of the American Control Conference, Boston, MA, pp. 1661–1666.