Contents lists available at ScienceDirect

Chemical Engineering Research and Design

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

Operational safety via model predictive control: The Torrance refinery accident revisited

Zhihao Zhang[a], Zhe Wu[a], David Rincon[a], Panagiotis D. Christofides[a,b,*]

[a] Department of Chemical and Biomolecular Engineering, University of California, Los Angeles, CA 90095-1592, USA
[b] Department of Electrical and Computer Engineering, University of California, Los Angeles, CA 90095-1592, USA

ARTICLE INFO

Article history:
Received 12 June 2019
Received in revised form 27 June 2019
Accepted 1 July 2019
Available online 12 July 2019

Keywords:
Operational safety
Process control
Model predictive control
Nonlinear processes
Fluid catalytic cracking process

ABSTRACT

An accidental explosion at the refinery operated by ExxonMobil in Torrance, California occurred in 2015 during operation at the Safe Park mode via the operations and integrity management system (OIMS) is analyzed in this work, and a control-based approach is presented for how the accident could have been potentially avoided. Specifically, this work reproduces and tackles the accident in Torrance, California in 2015 by dynamical modeling of the fluid catalytic cracking (FCC) unit that played a key role during the accident using information extracted from the final investigation report. A model predictive controller with an offset-free mechanism is proposed and is applied to the process under two different scenarios. The first scenario is based directly on the accident in the report in Torrance, California in 2015, while the second scenario is another potentially catastrophic situation that could have occurred. The obtained results in Aspen Plus Dynamics demonstrate that the proposed safety-aware control system is able to avoid the accident under both scenarios.

1. Introduction

On Wednesday, February 18, 2015, an accidental explosion in the gasoline processing unit at the refinery operated by ExxonMobil in Torrance, California took place involving mainly the following units: a distillation column, a fluid catalytic cracking (FCC) unit, and an electrostatic precipitator (ESP). The explosion led to an economic loss, which is estimated to be from $2.4 up to $6.9 billions, and caused harm on health of operators and people surrounding the refinery (CSB, 2017a; Gonzales et al., 2016). Based on the transcripts of the public meeting about the accident in Torrance, California (CSB, 2017a), ExxonMobil used a methodology named operations and integrity management system (OIMS) for its process safety system, which was found to be defective in that it lacks a hierarchy inspection of control analysis and an implementation of safeguards from process hazard analysis (CSB, 2017a). It was further suggested by the final report from Chemical Safety Board (CSB) that a controller should be incorporated in the Safe Park mode (CSB, 2017b). It is worth quoting directly from that report: "*ExxonMobil did not develop a Safe Park procedure for how to safely operate within specified safe operating limits, with specified operating parameters that could directly verify the critical Safe Park safeguards. Safe Park procedure development and improved measurement and control of critical process conditions could have prevented this incident.*"

Despite the economical, the environmental, and the overall casualty rate involved in such accidents, most chemical processes still rely on process safety studies such as hazard and operability analysis (HAZOP), hazard identification (HAZID) and layer of protection analysis (LOPA) (Zhang et al., 2019a). However, in a paper presented in the conference of society of petroleum engineers on health, safety, environmental, and social responsibility in 2018, the limitations of implemented safety studies in the industry and their link with the accidents were pointed out (Godfrey et al., 2018). For instance, the ExxonMobil refinery in Torrance, and other involved plants

* *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.2019.07.002

investigated by US Chemical Safety Board (CSB) were used as references to show that common safety studies, such as HAZOP and HAZID, lead to the recurrent triggers of different accidents (Godfrey et al., 2018).

The key problem of HAZOP, LOPA and HAZID and similar process safety techniques is that they were proposed more than a half century ago, which do not adapt to the current industrial operations (Godfrey et al., 2018). These process safety techniques are open-loop analysis techniques without real-time feedback, and they do not use real-time information during the operation. Moreover, process dynamics is not taken into account in these traditional techniques. Recently, some efforts have been made to investigate the disadvantages of traditional safety techniques and to improve the current practices. For example, an accident at the BP refinery in Texas in 2005 was investigated with a dynamic simulation tool to better understand the column flooding and overfilling (Manca and Brambilla, 2012; Isimite and Rubini, 2016). In this dynamic HAZOP approach, a dynamic simulator is integrated with the traditional HAZOP study in order to reduce the speculation while identifying the relevant events. In Kummer and Varga (2019), it is argued that HAZOP has not changed at the same pace as industrial technology, which has been more integrated nowadays, especially with more frequent changes in set-point during normal operations (e.g., when using economic model predictive control). For that reason, identifying all potential events that can lead to an accident in the process becomes difficult using the HAZOP approach only. Similarly, common process safety frameworks lack of well-known control properties in their formulations as was pointed out, for example, in the defense-in-depth strategy, which has been applied in the nuclear industry for safety studies (Saleh et al., 2014).

Recently, some research works have been done on the integration of process safety systems with process control systems for real-time operation of industrial processes (Zhang et al., 2019a). For instance, a high-pressure flash drum with its safety device and an MIC reactor associated with the Bhopal incident were studied using a control methodology that allows to avoid operating in unsafe regions (Zhang et al., 2018). Additionally, a multi-unit ammonia process which integrates safety constraints and model predictive control was tested under a disturbance that is associated with reaction thermal runaway in a co-simulation of Matlab and Aspen Plus Dynamics (Zhang et al., 2019a,b).

In this direction, this study develops a model predictive control system for the FCC unit. Specifically, the accident in Torrence, California is studied in detail by following closely the findings and suggestions in the report from CSB. Then, after identifying the trigger events and operation conditions during the accident, the FCC unit is simulated in Aspen Plus Dynamics. In order to avoid the incident, we follow the suggestion by the CSB report and develop a model predictive controller using the recommended safeguards in the Safe Park mode. In addition, offset-free control technique is combined with the MPC such that the controlled variables are driven to the set-point without offset. Since any potential offset can cause severe dangers in the case of significant disturbances, offset-free methodology is employed in the controller, as discussed in Wallace et al. (2016). Finally, two sets of disturbances are introduced into the FCC unit to demonstrate the effectiveness of the proposed safety-aware control system.

The rest of the paper is organized as follows: in Section 2, the fluid catalytic cracking process is introduced with the main events that occurred during the accident at the refinery operated by ExxonMobil in Torrance, California. Then, the key aspects for dynamically simulating the refinery with the implementation of the disturbances that can cause the accidents are explained. In Section 3, the controller design is presented in which the model identification and the offset-free approaches are utilized in the control system. In Section 4, the simulation results are presented for the FCC unit under the proposed controller and the disturbances that trigger the same accident as in the CSB report.

2. Fluid catalytic cracking (FCC) process and accident description and modeling

Nowadays there are around 400 fluid catalytic cracking units operating around the world that are responsible for producing 45% of the naphtha worldwide among many other products (Pinheiro et al., 2011; Sildir et al., 2015). Four distinct designs have been developed for the FCC process since the first FCC unit started to operate in 1940s. Specifically, in 1947, UOP's stacked unit was the first to include the spent catalyst stripping idea in which the spent catalyst is driven by gravity (Pinheiro et al., 2011; Sildir et al., 2015). In 1952, FCC model IV was proposed by Standard Oil Development, in which a vessel is placed to the side of the reactor using U-bend connector for regenerating the catalyst (Pinheiro et al., 2011; Sildir et al., 2015). In 1979, by taking advantage of a new catalyst design and the Kellogg's Orthoflow F process (i.e., a two-step catalyst regeneration process), Exxon proposed the Flexicracking unit that uses a side-by-side concept in which the regenerator is placed in a lower position compared to the riser cracking reactor position (Pinheiro et al., 2011; Sildir et al., 2015). Finally, in 1981, Total Petroleum USA proposed a residue FCC unit, also named R2R unit, in which two regenerators are used allowing the reduction of the catalyst deactivation to a minimum level (Fernandes et al., 2007).

Following the design method in Pinheiro et al. (2011) and CSB (2017b), the following subsections describe the general FCC process, and then elaborate on the accident details in the explosion at the Torrance refinery. Aspen Plus Dynamics is used to model the FCC process with disturbances to simulate the accident conditions.

2.1. *Fluid catalytic cracking (FCC) process*

In this subsection, a simplified description of the FCC process is presented together with the key characteristics of each unit in the FCC process. Specifically, the FCC process involves a reactor, a riser, a catalyst regenerator, a distillation column, an expander and an electrostatic precipitator (ESP). A schematic of the FCC process network is shown in Fig. 1. The FCC unit cracks heavy, high boiling-point hydrocarbon molecules into smaller molecules with lower boiling points. The cracking reactions take place in the riser and the reactor. The distillation column is used to separate the hydrocarbon mixture from the reactor. The spent catalyst is regenerated in the regenerator by combustion with air. After that, the expansion of flue gas through an expander provides power to drive the air compressors. Finally, an ESP system is used to remove catalyst particles from the regenerator combustion gas to meet environmental regulations before it is discharged into the atmosphere.

In the riser, heavy hydrocarbons are mixed with hot catalyst and are cracked into smaller molecular weight com-

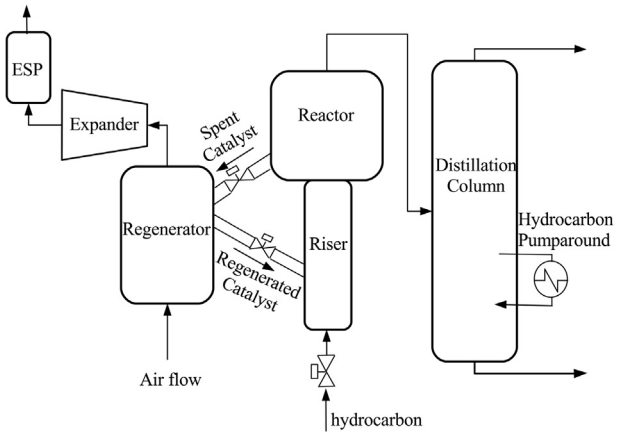


Fig. 1 – A schematic diagram of main units in FCC process under normal operation condition.

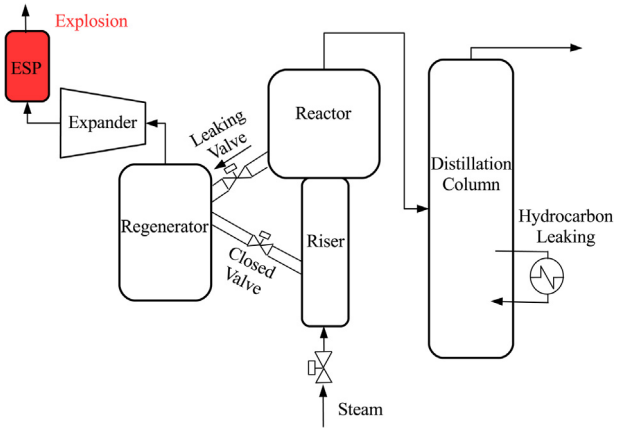


Fig. 2 – A schematic diagram of disturbances (valve leaking and hydrocarbon leaking) leading to the accident under Safe Park mode.

ponents. The cracked hydrocarbon vapor then flows to the distillation column for separation. During the cracking process, coke deposits onto the catalyst, deactivating the catalyst. Under normal operation, the catalyst circulates between the reactor and the regenerator, in which used catalyst moves from the reactor to the regenerator through the spent catalyst slide valve, while regenerated catalyst moves from the regenerator to the riser by the regenerated catalyst slide valve.

Leaving the top of the reactor, the superheated cracked hydrocarbon mixture enters the distillation column, with no additional heat added to the column under normal operation. Several pumparounds are used to remove heat from the column to cool and condense the vapor for separation. In these pumparounds, heat exchangers transfer heat to other process streams (usually hydrocarbon streams) in the refinery by reducing the temperature of the streams, and then returning to the distillation column. The distillation column separates the hydrocarbon mixture into light hydrocarbons, heavy naphtha, light cycle oil, and slurry oil.

Inside the regenerator, the coke on the surface of the hot catalyst particles burns off in a combustion reaction through contact with air. The exhausted gas leaves the top of the regenerator, containing combustion product gases with catalyst particles. Then, the flue gas flows through the gas/catalyst separator, expander, carbon monoxide boiler, and finally, the gas is routed to ESP. The expander uses expansion of gas to power other units in the process. The ESP collects most of the remaining small catalyst particles from the flue gas to meet California emissions regulations by using charged plates to attract the fine catalyst particles. This operation generates sparks, potentially leading to flame ignition inside of the ESP.

2.2. *Accident description*

Among the many issues involved during the 2015 accident, the key events that lead to the accident are described below, followed by the main conclusions of the accident investigation and the proposed solutions to avoid this incident in the future (CSB, 2017b). Before the explosion, the following sequential events occurred at the Torrance refinery: (1) The flue gas that flowed through the expander contained a small amount of catalyst particles that built up on the blades and caused vibrations in the expander. Several efforts were carried out to reduce the vibrations in the expander, ending up without significant improvement. (2) On February 16, 2015, the vibrations reached the high limit and the control system steered the plant to a "Safe Park" mode. (3) During the Safe Park mode, the following actions were taken: the spent catalyst valve and regenerated catalyst valve were closed to prevent gas flowing from the reactor to the regenerator; the hydrocarbon feed stopped; the expander was shut down; and steam was injected to the FCC to replace hydrocarbon. (4) However, the following failures occurred: the ESP remained energized to provide potential ignition; the spent catalyst valve failed to seal and maintain the desired level of catalyst, due to an eroded valve over the years; and a leaking heat exchanger in the pumparound allowed light hydrocarbons to enter the distillation column with a higher pressure. (5) Because there was steam leaking from the expander outlet flange when the workers were trying to repair the expander, the supervisor agreed to reduce the steam flow from 20,000 pounds per hour to 7500 pounds per hour, which is still higher than the minimum flow rate of 2000 pounds per hour reported on the safety instructions. (6) The reactor pressure was too low to prevent hydrocarbons from backflowing from the distillation column into the reactor. Around one hour later, alarms indicated that hydrocarbon was leaking and the flammable mixture ignited inside of the ESP, causing an explosion.

As shown in Fig. 2, the involved units in the refinery are the fluid catalytic cracking unit, the distillation column and the electrostatic precipitator. Based on the CSB final report for the distillation column, the engineers used two safeguards to prevent the backflow from the column to the FCC. The first safeguard was to maintain a positive pressure difference between the reactor and the distillation column. The second safeguard was to maintain a physical barrier between the reactor and regenerator by closing the spent catalyst valve and accumulating catalyst above the valve. Moreover, in order to monitor the above two safeguards, the engineers used indirect variables as indicators. For the first safeguard, the spent catalyst slide valve position was used to indicate that the catalyst accumulates above the valve and forms a barrier between regenerator and reactor; however, it was pointed out in the report that using a direct indicator is more effective as, for example, the catalyst level. The second indirect variable used by the engineers to check the pressure difference between the reactor and the distillation column was the steam flow rate, which was set to 2000 pounds per hour as the minimum flow rate of the steam feed to the reactor. Similarly, it was noted by the CSB report that using a differential pressure measurement is prudent for monitoring directly this key safeguard.

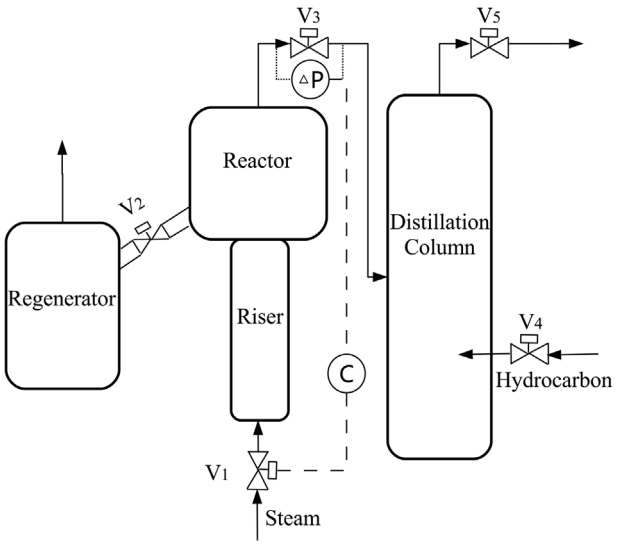


Fig. 3 – A schematic diagram of simulated units and control structure in the Aspen simulation.

One solution is to specify operation limits for all possible operation modes. By the time of the accident, engineers implemented a two-way mode that will permit to drive the process from normal operation to Safe Park mode, and vice versa. However, the implemented two-way mode did not define specific operation limits needed for maintaining the FCC safe when operating in Safe Park mode. Morever, the CSB report went further in its suggestion to indicate the need of implementing a closed-loop (feedback controlled) operation when the process is in Safe Park mode using the direct measurement variables for the safeguards as discussed before. It is mentioned in the report that the engineers could have implemented a process control system that automatically adjusts the steam flow rate in the reactor to maintain the target reactor/distillation column differential pressure in the Safe Park mode. Process operation limits could also be involved in the controller configuration to avoid the accident.

2.3. *Aspen dynamic model*

In order to accurately simulate the process dynamics and interaction among the FCC units, Aspen Plus and Aspen Plus Dynamics V10.0 (Aspen Technology, Inc.) are used to perform high-fidelity dynamic simulation of the FCC process. Aspen Plus is a commercial software that calculates the steady-state of the process given a process design and an appropriate selection of thermodynamic models, based on the mass and energy balances of the process using a sequential modular approach. Aspen Plus Dynamics is another software that can run dynamic simulations based on steady-state model data and additional detailed parameters. Further details about Aspen software can be found in Al-Malah (2016) and Aspen Technology Inc. (2003).

In our simulation, the components are water and pentane. Water is the component in the vapor steam, and pentane is a typically involved hydrocarbon in the FCC unit. As shown in Fig. 3, the Aspen model includes a riser, reactor, regenerator, distillation column and five valves. The reactor riser is a tube reactor with 1 m diameter and 30 m height. The reactor is a homogeneous one with 3 m diameter and 30 m height. The distillation column in our simulation is a homogeneous reactor with 4 m diameter and 50 m height. The regenerator is a homogeneous reactor with 6 m diameter and 40 m height.

The following general forms of the mass balance, energy balance and momentum balance equations in Aspen Plus Dynamics are used to dynamically simulate the above process (without reaction in the Safe Park mode):

$$\frac{\partial}{\partial t}(\rho\omega_i) = -(\nabla \cdot n_i) \tag{1}$$

$$\frac{\partial}{\partial t}(\rho v) = -[\nabla \cdot \Phi] \tag{2}$$

$$\frac{\partial}{\partial t}\rho(\hat{U} + \frac{1}{2}v^2) = -(\nabla \cdot e) \tag{3}$$

where ρ is the total density, ω_i is the mass fraction of component i, n_i is the mass flux of component i, v is the velocity, Φ is the combined momentum-flux tensor, $\hat{U}$ is the internal energy per unit mass, $\frac{1}{2}v^2$ is the kinetic energy per unit mass, and e is the total energy flux. In addition to equations reflecting the mass, energy and momentum conservation laws, dynamic models also include system-dependent constitutive equations, which define the relationships between intensive variables such as thermal dynamic equation of state.

Additionally, the simulation involves 5 valves as shown in Fig. 3. Steam valve V_1 is the valve before the reactor riser, which is used to adjust the steam flow rate. The incoming steam to valve V_1 has a pressure of 150 psig and a temperature of 300 °C. Valve V_2 is the spent catalyst valve. Under Safe Park mode, valve V_2 should be able to close fully; however, it fails to seal during the accident. Valve V_3 is the valve between the reactor and the distillation column. The pressure drop of valve V_3 indicates the pressure barrier for the accident since hydrocarbon is less likely to backflow into the reactor under high positive pressure drop. The pressure drop value is usually small since this pressure drop is wasted during normal operation. Valve V_4 connects hydrocarbon and the distillation column. Valve V_4 keeps closed under normal condition and opens to simulate hydrocarbon leaking in the pumparound in the distillation column. Valve V_5 is the top valve of the distillation column, which only closes when there is a block on top of the distillation column. The size of all valves are carefully characterized such that the pressure in the reactor and the distillation column is consistent with the data in the CSB report under different conditions (CSB, 2017b).

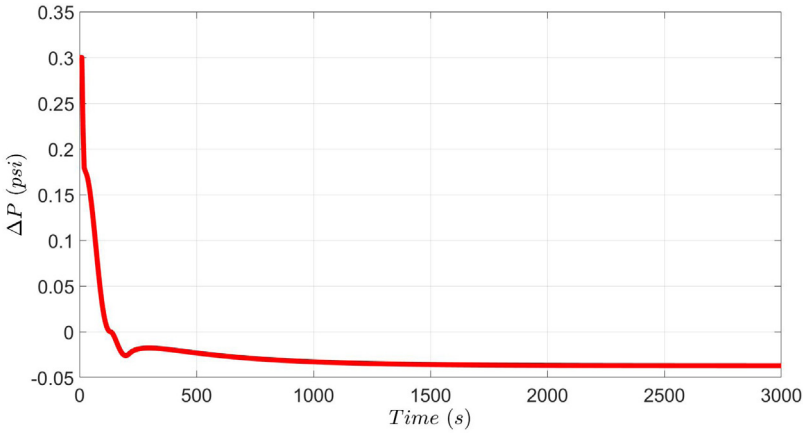
Flow rate through a valve is calculated by the following equation:

$$F^2M = \frac{1}{2}\left(\frac{Pos}{100}C_0^{max}\right)^2 \rho\Delta P \tag{4}$$

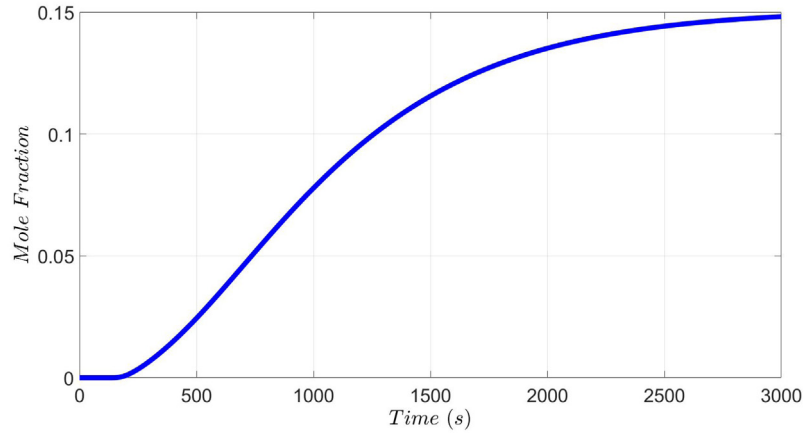
where F is molar flowrate in kmol/h, M is molecular weight in kg/kmol, Pos is valve position in %, C_0^{max} is maximum flow coefficient in $m^{1.5}\,kg^{0.5}\,h^{-1}\,bar^{-0.5}$, ρ is molar density in kmol/m^3, and ΔP is the pressure drop across the valve in bar.

2.4. *Disturbances leading to accident*

In the accident, the spent catalyst slide valve was leaking so that there was no catalyst barrier between the reactor and the regenerator. According to the final CSB report, it took about 10 min for the catalyst to leak in the spent catalyst valve. At the same time, it was reported that there was hydrocarbon leaking in distillation column which provides dangerous flammable hydrocarbon into the process. In order to investi-



(a) Pressure drop between reactor and distillation column



(b) Hydrocarbon mole fraction in the regenerator

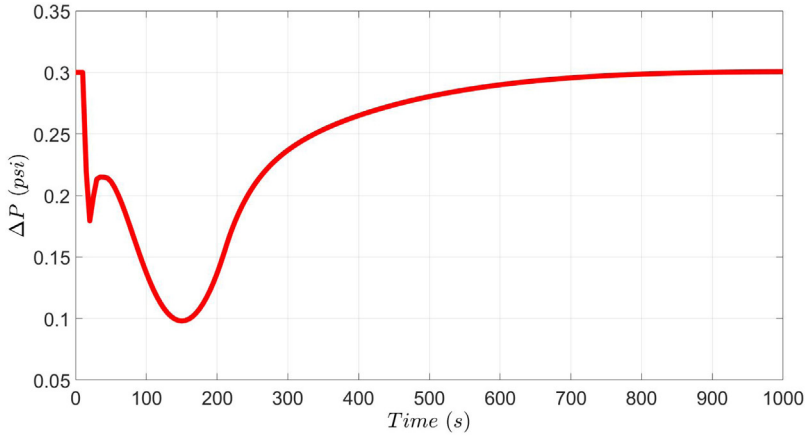
Fig. 4 – Open-loop simulation results under two disturbances.

gate more severe unsafe scenarios in the process, the top valve in the distillation column could be used for creating another potential danger. A high pressure in distillation column can be created by a blocked top valve, which potentially causes back flow of hydrocarbon from the distillation column to the reactor.

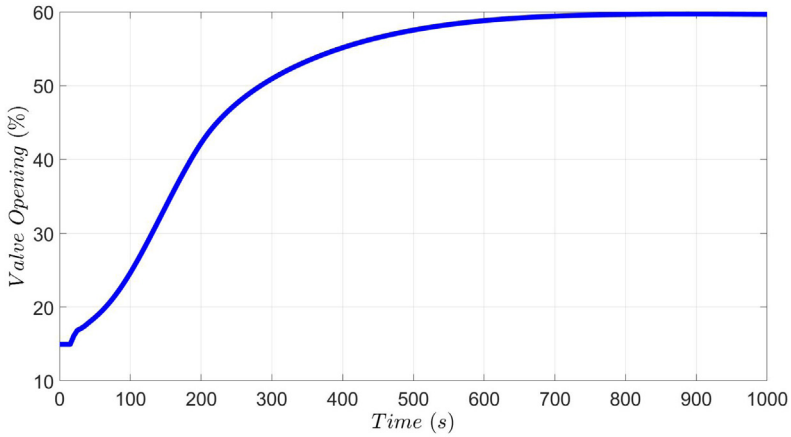
In our simulation, there is a valve V_2 between the reactor and the regenerator, which opens from 0% to 100% in 200 s to simulate the spent catalyst valve leaking. If the spend catalyst valve leaks faster, then the valve V_2 opens faster and creates a more dangerous situation. It is noted that although 200 s is faster than the actual time (8 min) in the accident, it can be regarded as a reasonable disturbance. To simulate hydrocarbon leaking in the distillation column, a hydrocarbon flow is connected to the distillation column with valve V_4, which opens from 0% to 100% in 5 s. Another disturbance in the simulation is located in the distillation column top valve V_5, which closes from 100% to 50% in 5 s in order to simulate the situation in which this top valve is blocked. If the distillation column top is blocked faster, then the valve V_5 closes also faster and requires the steam flow to increase more rapidly to maintain the desired pressure drop.

3. Model predictive controller design

Due to the fact that the FCC is highly interconnected with other units in the refinery and dealing with dangerous operating conditions (e.g., high temperature conditions in a range between 750 and 800 K) and explosive substances (e.g., gasoline and naphtha), it is challenging for engineers to predict the malfunction of the plant using information from safety procedures in manuals. When the accident occurred, hydrocarbon flows back from the distillation column into the reactor, which indicates that the pressure drop of valve V_3 is negative. In order to increase the pressure drop and rebuild the pressure barrier, the steam flow rate needs to be increased, or the steam valve V_1 needs to open more. Since implementing operation limits in open-loop cannot handle disturbances that are not known a priori, a feedback controller is needed to determine the sufficient valve opening in the actuator based on feedback measurements to ensure operational safety. Therefore, to avoid the above accident and other unsafe operations, a model predictive controller is developed for the FCC process. The controlled variable is the pressure drop of valve V_3 and the manipulated variable is the steam valve V_1 position, which adjusts the steam flow rate. It needs to be mentioned that the pressure drop of V_3 can indicate the pressure barrier and the occurrence of hydrocarbon back flow, and thus, it is used as a measured state. The steam flow rate is the main operating variable during the accident, and thus, the steam valve is chosen as manipulated in this paper. The described control loop in the FCC process is demonstrated in Fig. 3. It is noted that a PI controller could be used in this situation but it does not account for constraints or optimality. In our work, there is a constraint on the valve opening that is handled by the MPC. Additionally, the pressure drop needs to be kept positive with an optimal performance, and thus, a model predictive controller is used. Additionally, since the process model in MPC is identified from the nominal process, in order to achieve an



(a) Pressure drop between reactor and distillation column.



(b) Steam valve position

Fig. 5 – Closed-loop simulation results under two disturbances.

offset-free performance, an augmented (additional) state is used in the MPC to eliminate any potential offset.

3.1. *Data-driven process model*

The fluid catalytic cracking process is initially simulated at its steady-state with steam valve position $Pos_{ss} = 14.96\%$. The pressure drop between the reactor and the distillation column at steady-state is $\Delta P_{ss} = 0.3$ psi. The state and the input of the process are represented in deviation variable form as $x = \Delta P - \Delta P_{ss}$ and $u = Pos - Pos_{ss}$, such that the equilibrium point of the system is at the origin. It is demonstrated that the use of a linear model in MPC with the implemented offset-free technique works well in the current work. Therefore, a nonlinear model is not necessary to be used in the MPC since it requires more calculations to identify the nonlinear model and to solve the MPC optimization problem in real-time. The following linear state-space model is used to describe the relationship between pressure drop and valve position:

$$\dot{x} = Ax + Bu \tag{5}$$

where x is the state variable, u is the manipulated input variable, and the parameters A and B are identified using Aspen simulation data. Specifically, data on pressure drop ΔP are generated from the nominal open-loop simulations with pseudorandom binary sequence (PRBS) signal in valve position Pos. Then, the Multivariable Output Error State Space (MOSEP) algorithm is applied in Matlab to identify the parameters A and B as follows:

$$A = -0.304; \quad B = 0.0102.$$

In order to handle plant-model mismatch in MPC, an additional state θ is incorporated into the model of Eq. (5). The additional state θ is assumed to be constant and the model is augmented as shown in Eq. (6):

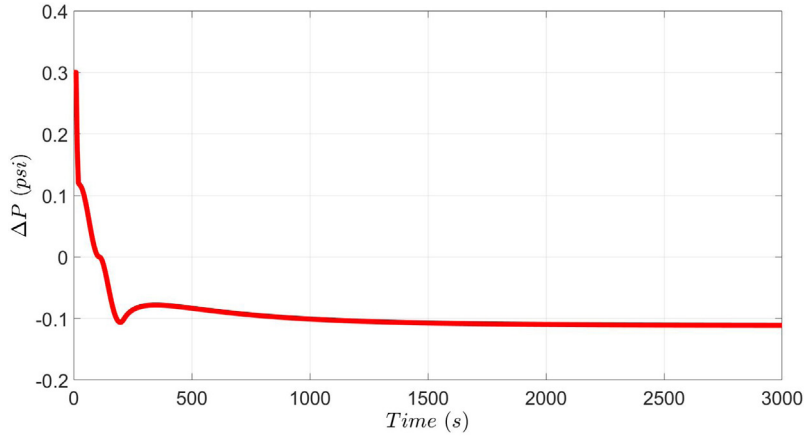
$$\begin{aligned} \dot{x} &= Ax + Bu + G_\theta \theta \\ \dot{\theta} &= 0 \end{aligned} \tag{6}$$

In the presence of the augmented state θ, an observer is designed to estimate the full state as follows:

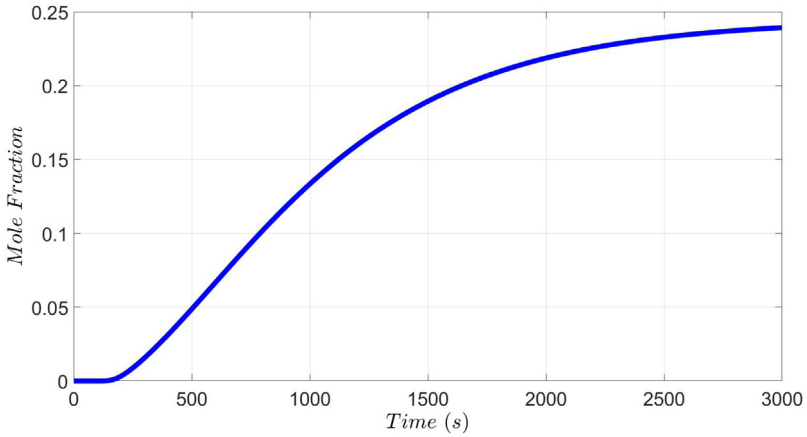
$$\begin{aligned} \dot{\hat{x}} &= A\hat{x} + Bu + G_\theta \hat{\theta} + L_x(x - \hat{x}) \\ \dot{\hat{\theta}} &= L_\theta(x - \hat{x}) \end{aligned} \tag{7}$$

where $\hat{x}$ and $\hat{\theta}$ are the variables of the state observer and x is the actual state measurement. To apply the continuous observer in a sample-and-hold fashion, the estimated state $\tilde{x}(t_k)$ and $\tilde{\theta}(t_k)$ at sampling time t_k is calculated numerically from the last estimated state $\tilde{x}(t_{k-1})$ and $\tilde{\theta}(t_{k-1})$ using the Eq. (7), integrated with the explicit Euler method. The initial estimated states are set to be zero $\tilde{x}(0) = 0$ and $\tilde{\theta}(0) = 0$.

L_x and L_θ are the observer gain parameters. Observer error $e = \begin{bmatrix} x - \hat{x} \\ \theta - \hat{\theta} \end{bmatrix}$ and $\dot{e} = \begin{bmatrix} \dot{x} - \dot{\hat{x}} \\ \dot{\theta} - \dot{\hat{\theta}} \end{bmatrix} =$



(a) Pressure drop between reactor and distillation column.



(b) Hydrocarbon mole fraction in the regenerator

Fig. 6 – Open-loop simulation results under three disturbances.

$$\begin{bmatrix} A(x-\hat{x})+G_\theta(\theta-\hat{\theta})-L_x(x-\hat{x}) \\ -L_\theta(x-\hat{x}) \end{bmatrix} = \begin{bmatrix} A-L_x & G_\theta \\ -L_\theta & 0 \end{bmatrix} \begin{bmatrix} x-\hat{x} \\ \theta-\hat{\theta} \end{bmatrix}.$$

To ensure that the observer error $e(t) \to 0$ as $t \to \infty$, parameters L_x, L_θ and G_θ are chosen such that matrix $\begin{bmatrix} A-L_x & G_\theta \\ -L_\theta & 0 \end{bmatrix}$ is Hurwitz. In our simulation, the parameters are chosen to be:

$$L_x = -0.3; \quad L_\theta = 0.8; \quad G_\theta = 0.02$$

3.2. *Offset-free MPC design*

The augmented state estimates from Eq. (7) are used to initialize the following offset-free MPC optimization problem:

$$\min_{u \in S(\Delta)} \int_{t_k}^{t_{k+N}} (\|\tilde{x}(\tau)\|^2_{Q_c}) \, d\tau \tag{8a}$$

$$\text{s.t.} \quad \dot{\tilde{x}} = A\tilde{x} + Bu + G_\theta\tilde{\theta}; \quad \dot{\tilde{\theta}} = 0 \tag{8b}$$

$$\tilde{x}(t_k) = \hat{x}(t_k); \quad \tilde{\theta}(t_k) = \hat{\theta}(t_k) \tag{8c}$$

$$u(t) \in U, \quad \forall \ t \in [t_k, t_{k+N}) \tag{8d}$$

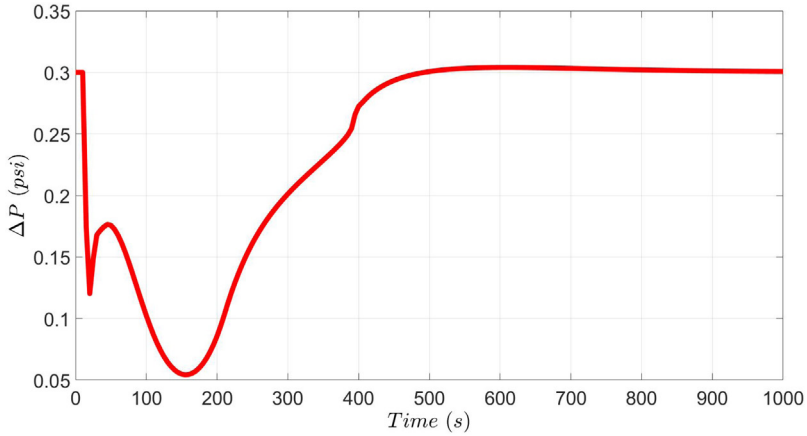
The objective function of Eq. (8a) requires minimizing $\int_{t_k}^{t_{k+N}} (\|\tilde{x}(\tau)\|^2_{Q_c}) \, d\tau$ so that the predicted state $\tilde{x}$ can be driven to the set-point (i.e., $x = 0$). The key reason for not minimizing u in the cost function is that $u = 0$ is no longer the steady-state corresponding to $x = 0$ in the presence of unknown disturbance and it is impossible to calculate the new steady-state u. Besides, it allows the controller to respond faster if the manipulated input is not penalized in the cost function. The constraint of Eq. (8b) is the full-state linear model of Eq. (6) that is used to predict future states in the objective function. Eq. (8c) defines the initial condition $\tilde{x}(t_k)$ and $\tilde{\theta}(t_k)$ of the optimization problem as the state observer value $\hat{x}(t_k)$ and $\hat{\theta}(t_k)$ at $t = t_k$, which are calculated by Eq. (7) with explicit Euler method using the measured state x and previously estimated states $\tilde{x}(t_{k-1})$ and $\tilde{\theta}(t_{k-1})$. Eq. (8d) is the input constraint applied over the entire prediction horizon. The manipulated input is the valve position *Pos*, which is bounded by: $0\% \leq Pos \leq 100\%$, namely $U = [-14.96, 85.04]$.

The explicit Euler method with an integration time step of $h_c = 10^{-3}$ s is applied to numerically integrate the dynamic model of Eq. (6) in MPC optimization problem. The nonlinear optimization problem of MPC of Eq. (8) is solved using the solver FilterSD on OPTI Toolbox in Matlab with the following parameters: sampling period $\Delta = 5$ s; and prediction horizon $N = 20$.

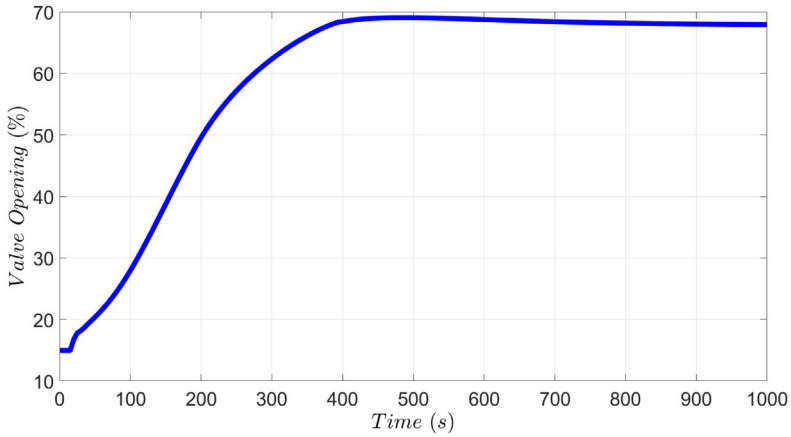
4. Closed-loop simulation results and discussion

4.1. *Two disturbances*

In order to simulate the accident conditions, the following disturbances are introduced: (1) spent catalyst valve V_2 opens from 0% to 100% from $t = 10$ s to $t = 210$ s; (2) valve V_4 opens from 0% to 100% from $t = 10$ s to $t = 15$ s. Fig. 4 shows the open-loop simulation. After introducing disturbances, the pressure drop



(a) Pressure drop between reactor and distillation column.



(b) Steam valve position

Fig. 7 – Closed-loop simulation results under three disturbances.

decreases from 0.3 psi to −0.04 psi. A negative pressure drop means that hydrocarbon flows from the distillation column to the reactor (i.e., backflow). Then, if the spent catalyst valve fails, hydrocarbon can flow into the regenerator and potentially causes damage in downstream units. In our simulation, when the spent catalyst fails, the obtained mole fraction of pentane in the regenerator outlet flow reaches 0.15, which is much higher than the explosion limit of pentane (0.015–0.078). Since other components in naphtha have similar explosion limit, mole fraction of 0.15 can cause an explosion in the ESP. In order to avoid this dangerous operation condition, the designed controller is applied to this situation.

The designed controller is applied to the process and the closed-loop simulation results are shown in Fig. 5. The pressure drop initially decreases as a result of the disturbance. Then, the steam valve starts to open to allow more steam flow to ensure safety of the process. At each sampling time t_k, the observer estimates the states $\tilde{x}(t_k)$ and $\tilde{\theta}(t_k)$ by Eq. (7) using the measured state x and previously estimated states $\tilde{x}(t_{k-1})$ and $\tilde{\theta}(t_{k-1})$. Since the disturbances decrease the pressure drop, the measured state x is less than the estimated $\hat{x}$. Then, a negative value $\hat{\theta}$ is calculated from Eq. (7) and is used in the model (Eq. (8b)) for prediction in the MPC. A negative θ on the right hand side of Eq. (8b) requires a further positive input u to bring the state $\tilde{x}$ back to the steady-state, which opens the steam valve position to feed more steam into the process. The augmented state θ keeps changing until there is no difference between x and $\hat{x}$, and as a result, the MPC drives the state x back to the steady-state without offset. The use of θ makes the controller to request further opening of the steam valve in the unsafe scenario until the pressure drop comes back to its steady-state value. Therefore, as shown in Fig. 5, the valve keeps opening and the pressure drop stops decreasing at around 150 s and goes back to 0.3 psi at the end of the simulation without offset. The pressure drop curve in Fig. 5a is not smooth because the introduced disturbance changes abruptly.

Additionally, it is important to note that there is not backflow under the implemented disturbances and the proposed safety-aware control system. As a matter of fact, the pressure drop has never been negative during the entire simulation, and therefore, there is no hydrocarbon flow from the distillation column to the regenerator after introducing the disturbance. The proposed controller can then be applied to the FCC process in order to operate the units safely while in Safe Park mode, as suggested in the accident report in Torrence, California (CSB, 2017b).

4.2. *Three disturbances*

In order to demonstrate that the designed controller can be applied in various unsafe conditions, additional disturbances are introduced as follows: (1) spent catalyst valve V_2 opens from 0% to 100% from $t = 10$ s to $t = 210$ s; (2) valve V_4 opens from 0% to 100% from $t = 10$ s to $t = 15$ s; (3) the distillation column top valve V_5 closes from 100% to 50% from $t = 10$ s to $t = 15$ s. Fig. 6 shows the open-loop simulation for these disturbances. After introducing these three disturbances, the pressure drop decreases from 0.3 psi to −0.11 psi, which is more negative than the two disturbances case. A negative pressure drop indicates that hydrocarbon flows from the

distillation column to the reactor and regenerator, and potentially causes damage in the downstream units as well. In this simulation, the mole fraction of pentane in the regenerator outlet flow reaches about 0.255 in the regenerator, which is much higher than the explosion limit and can cause a potential explosion in the ESP. The proposed controller is then applied to this situation to evaluate how the controller can deal with operational safety issues under these three disturbances.

The designed controller is applied to the process and the closed-loop simulation results are shown in Fig. 7. The pressure drop decreases at the beginning as a response to the disturbances. Then, the controller calculates an increasing input to open the steam valve. Therefore, the pressure drop starts to increase after reaching the minimum value of 0.05 psi, and finally, goes back to 0.3 psi without offset. Since there are more disturbances in this situation, the steam valve opens to a larger position 68% compared to 60% in the two disturbance case. Again, the pressure drop has never been negative during the simulation, which implies there is no hydrocarbon backflow after introducing the disturbances. This simulation demonstrates that the proposed controller can be applied to the FCC process in the presence of unexpected additional disturbances.

5. Conclusion

In this work, we demonstrated that process operational safety was improved with an offset-free model predictive controller to avoid a fluid catalytic cracking process accident, which occurred in the refinery operated by ExxonMobil in 2015 in Torrance, California. A dynamic simulation was developed in Aspen Plus Dynamics to emulate the essential units of the fluid catalytic cracking process. Disturbances were introduced to the process to simulate the accident conditions taken from the final report of the CSB and other dangerous situations with unexpected disturbances. An MPC with augmented state to obtain offset-free performance was designed to improve the process operational safety in order to avoid the accident and other potential dangerous scenarios. Closed-loop simulations demonstrated that the accident could have been avoided with the proposed controller under the reported accident condition and other potential dangerous situations.

Acknowledgments

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

References

Al-Malah, K.I., 2016. Aspen Plus: Chemical Engineering Applications. John Wiley & Sons.
Aspen Technology Inc, 2003. Aspen Plus User Guide. Aspen Technology Inc., Cambridge, MA.
CSB, 2017a. ExxonMobil Presentation: Transcript from 1.13.2016 Public Meeting. https://www.csb.gov/exxonmobil-refinery-explosion-/.
CSB, 2017b. ExxonMobil Torrance Refinery Final CSB Investigation Report. https://www.csb.gov/exxonmobil-refinery-explosion-/.
Fernandes, J.L., Verstraete, J.J., Pinheiro, C.I., Oliveira, N.M., Ribeiro, F.R., 2007. Dynamic modelling of an industrial R2R FCC unit. Chem. Eng. Sci. 62, 1184–1198.
Godfrey, M., et al., 2018. Implementing continuous improvement in hazard studies. In: SPE International Conference and Exhibition on Health, Safety, Security, Environment, and Social Responsibility, Society of Petroleum Engineers.
Gonzales, D., Gulden, T.R., Strong, A., Hoyle, W., 2016. Cost-Benefit Analysis of Proposed California Oil and Gas Refinery Regulations. Rand Corporation.
Isimite, J., Rubini, P., 2016. A dynamic HAZOP case study using the Texas City refinery explosion. J. Loss Prev. Process Ind. 40, 496–501.
Kummer, A., Varga, T., 2019. Process simulator assisted framework to support process safety analysis. J. Loss Prev. Process Ind. 58, 22–29.
Manca, D., Brambilla, S., 2012. Dynamic simulation of the BP Texas City refinery accident. J. Loss Prev. Process Ind. 25, 950–957.
Pinheiro, C.I., Fernandes, J.L., Domingues, L., Chambel, A.J., Graca, I., Oliveira, N.M., Cerqueira, H.S., Ribeiro, F.R., 2011. Fluid catalytic cracking (FCC) process modeling, simulation, and control. Ind. Eng. Chem. Res. 51, 1–29.
Saleh, J.H., Haga, R.A., Favarò, F.M., Bakolas, E., 2014. Texas City refinery accident: case study in breakdown of defense-in-depth and violation of the safety-diagnosability principle in design. Eng. Fail. Anal. 36, 121–133.
Sildir, H., Arkun, Y., Canan, U., Celebi, S., Karani, U., Er, I., 2015. Dynamic modeling and optimization of an industrial fluid catalytic cracker. J. Process Control 31, 30–44.
Wallace, M., Pon Kumar, S.S., Mhaskar, P., 2016. Offset-free model predictive control with explicit performance specification. Ind. Eng. Chem. Res. 55, 995–1003.
Zhang, Z., Wu, Z., Durand, H., Albalawi, F., Christofides, P.D., 2018. On integration of feedback control and safety systems: analyzing two chemical process applications. Chem. Eng. Res. Des. 132, 616–626.
Zhang, Z., Wu, Z., Rincon, D., Christofides, P.D., 2019a. Operational safety of an ammonia process network via model predictive control. Chem. Eng. Res. Des. 146, 277–289.
Zhang, Z., Wu, Z., Rincon, D., Garcia, C., Christofides, P.D., 2019b. Operational safety of chemical processes via safeness-index based MPC: two large-scale case studies. Comput. Chem. Eng. 125, 204–215.