MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Safety-centered process control design based on dynamic safe set

Joshiba Ariamuthu Venkidasalapathy*, Costas Kravaris, M. Sam Mannan
Artie McFerrin Department of Chemical Engineering,
Texas A&M University
College Station, Texas 77843-3122, USA
*Presenter E-mail: joshvenkat03@tamu.edu, kravaris@tamu.edu

Abstract

Despite significant efforts to make operation of chemical plants safer, the occurrence of incidents clearly indicates the need for better design approaches. Studies to identify the root causes of incidents in hydrocarbon industries reveal that poor design and inadequate control systems contribute to more than 20% of the offshore incidents[1] and 30% of the thermal runaway incidents [2] analyzed. Characterizing and quantifying process safety performance is a complex problem. Traditional control engineers used the concept of phase margin and gain margin to measure the stability of single feedback loops. Although it can be viewed as a measure of safety, the method does not account for multiloop interactions and the presence of constraints in the system. More recently, researchers have used model predictive control (MPC) theory to address safety concerns. The objective of the MPC optimization problem is maximization of cost and other performance metrics, where safety is modelled as a set of additional constraints that must be enforced. The approach is not adequate as there is not a clear method to quantify the safety performance for application in design. Process safety engineering concepts emerge from cause-effect based analysis like HAZOP analysis, fault trees and event trees. These methods do not account for multivariable and non-linear interactions. The objective of this research is to develop an approach for the process control problem with safety as the primary target.

In this paper, the concept of dynamic safe set (DSS) is formulated. The DSS is a set of states of the process that guarantee enforcement of safety critical constraints, in the presence of bounded safety threatening disturbances. Already existing mathematical concepts from the systems literature, namely maximal output admissible sets [3, 4] and the reference governor theory[5, 6] are used for evaluating the DSS. The DSS is calculated around a steady-state operating point. It is safe in the sense that if the initial state belongs to the DSS, then for all modeled disturbances the closed-loop system is guaranteed to not violate the constraints at any time in the future. The safety threatening disturbances that can increase the possibility of safety constraint violation by pushing the system to a risky operation zone are also modeled while calculating the DSS.

A method to quantify the size of the DSS is also proposed by defining the concept dynamic safety margin (DSM). It is defined as the minimum distance of the steady-state operating point from the boundary of DSS. The DSM margin is relevant and important because it is not possible to model

all possible disturbances. That is, a DSS with larger DSM will be able to handle unmodeled random disturbances that push the states away from the steady-state. This will be used as a safety performance metric for control system design. This will lead to designing processes with safety as the primary objective and all other performance metrics are treated as secondary considerations.

The DSS approach is also extended to applications in abnormal event management. Under upset scenarios, there is often a need for sudden and large set-point changes. To safely respond to those changes, control strategies need to be designed to stay away from the safety critical constraints. For this purpose, the concept of reference governor is used. The reference governor is a supervisory nonlinear control scheme that works along with an existing closed-loop system.

The DSS approach is tested on an exothermic process in a CSTR. The approach helped in selecting the operating condition of the process by identifying steady-states that are relatively safer. The closed loop process design was studied under proportional (P) and proportional-integral (PI) control strategies. It showed that the controller parameters played a significant role on the DSM of the process. The trade-off between control and safety performance can be analyzed using the DSM concept. The effect of maximum available control input on the system's safety performance was also investigated. The reference governor was also implemented to the CSTR. The dynamic responses of the process under large disturbances, demonstrate significantly superior control performance when compared to the process without reference governor.

1 Introduction

Ensuring safe operation is critical in chemical industries considering the potential consequences of incidents to life, environment and equipment. Traditional safety engineering concepts emerge from cause-effect based analysis like HAZOP analysis, fault trees and event trees [1-4]. The causation models used as the basis for developing process safety engineering tools have their limitations. These methods fail to account for multivariable and non-linear interactions, oversimplifying the incident process by using only direct cause-effect relations. Studies on incidents in process industries reveal that poor design and inadequate control systems contribute to more than 20% of the offshore incidents [5] and 30% of the thermal runaway incidents [6] analyzed. The objective of this paper is to change the way the process control design problem is approached by bringing process safety upfront.

Process safety can be encompassed within the systems engineering framework by representing it as a set of constraints that have to be met, failing of which may lead to undesirable consequences. These safety critical constraints are the pivotal elements of process safety and they must be chosen to prevent the loss of containment of flammable chemicals. They are conditions that ensure safe operation of the plant without compromising the integrity of the process. Examples of such constraints include limits on liquid level in vessels and bounds on pressure and temperature of columns. Constraints such as limits on available control input should be included as they determine the system's ability to be resilient. In addition to considering constraints that are restricted to individual units, it is important to incorporate constraints that account for the system as a whole, such as the overall energy and mass balance of the plant. A comprehensive set of safety critical constraints, when carefully chosen, can capture the safe region of operation for the process and hence will be used in the design and control problem.

A few researchers have adopted a system-theoretic perspective of addressing process safety as a set of constraints. In the context of safety, Model Predictive Control (MPC) theory is often used as a tool to incorporate the constraints in real-time implementation [7]. MPC computes control

actions for the manipulated inputs by solving dynamic optimization problems in real-time and takes advantage of the process model while accounting for constraints. Ensuring closed-loop stability, feasibility and performance under MPC along with safe operation is challenging and has only been explored recently [8-10]. It is important to note that MPC allows for operating the process while riding by the safety critical constraints as it focusses mainly on maximizing the objective function. This may push the process operation closer to unsafe region, increasing the risks. As a result, the need to bring safety as the primary objective of the process control design problem is critical.

The use of MPC for integrating safety constraints and proposed conditions that are required to be satisfied for effective control of safety constraints was proposed in [7]. Lyapunov-based MPC (LMPC) schemes that could drive the closed-loop state to a safe operating region (defined via Lyapunov level sets), where safety is ensured at a prescribed rate in the presence of small process uncertainties was developed in [11]. However, for large disturbances the Safety-LMPC does not guarantee operation in safe region. The safe region represented by Lyapunov level sets can also be restrictive. A safeness index was developed in [12] to represent safe region of operation and used it as a hard constraint while implementing MPC. They demonstrated guaranteed closed-loop stability for sufficiently small disturbances. However, the approach does not guarantee closed-loop stability and feasibility of the optimization problem for large disturbances. In [13], a model-based proactive safety system that incorporates safety constraints in the framework was developed. They used the safety constraints to perform real-time receding-horizon operability analysis to detect operation hazards. Unlike MPC, they are computationally less expensive. However, they can only detect the inadequacy in the control system's manipulated variable and was not capable of taking necessary corrective action. The above works aim to model safety constraints in the design of process control systems, but their limitations clearly indicate the need for a holistic approach.

In this paper, the concept of dynamic safe set (DSS) is proposed to capture the essence of safety critical constraints. The DSS is defined as a set of process states that guarantee the enforcement of safety critical constraints, in the presence of unknown safety threatening disturbances. It is a closed set that is calculated around a steady state operating condition. Already existing mathematical concepts from the systems literature, namely maximal output admissible sets and the reference governor theory are used for evaluating the DSS. A meaningful method to quantify the size of the DSS is proposed via the concept called dynamic safety margin (DSM). It is defined as the minimum distance of the steady state operating condition from the boundary of the DSS. This will be used as a measure of safeness of processes for designing safer systems. The potential applications of the DSS and DSM concepts in process control design are proposed in this paper. This will lead to designing processes with safety as the primary design objective with all other performance metrics treated as secondary considerations.

The paper is organized as follows: in section 2 the dynamic safe set approach is discussed; the brief and necessary overview of the mathematical concepts required to calculate the dynamic safety sets (DSS) is provided in section 3 along with the proposed definition and calculation procedure for the dynamic safety margin (DSM); the proposed DSS and DSM applications in designing the safer process control system is outlined in section 4; the proposed approach is implemented on the T2 Laboratories exothermic reaction handled in a continuous stirred tank reactor (CSTR) in section 5; lastly, in section 6, conclusions and future directions are discussed.

2 The Dynamic Safe Set (DSS) Concept

The primary objective of the proposed approach is to reformulate the process design and control problem bringing safety upfront. In this paper, safety is represented as a set of safety critical constraints that must be met. Integrating the safety constraints during the design phase has the advantage of minimizing hazards by choosing safer operating conditions, controller strategies and adequate equipment design. The first challenge is to identify a meaningful way to characterize and evaluate the process safeness, that is, a measure of how safe the design is. In this paper, process safety is viewed as a measure of the resilience of the process against disturbances. It is viewed as the ability of the process to return to its normal operating condition in the presence of disturbances and upsets while also respecting the physical constraints that must be satisfied.

A concept called dynamic safety sets (DSS) is formulated to characterize the process safeness. As its name suggests the DSS is a collection of states of the process that guarantees the enforcement of safety critical constraints at any point of time in the future. The safety critical constraints are such that they must be satisfied at all times, failing of which may result in serious consequences. The DSS will be determined around a steady state operating condition. If the process state is found to be away from the steady state operating point but within the DSS, then it is guaranteed that the system can be brought to the necessary steady state safely. The transient states that return the process from the disturbed condition to the steady state operating point, will also lie within the DSS; hence the set will be called the *dynamic* safe set. In the proposed work, the DSS will be evaluated for multi-dimensional systems with safety critical constraints while also accounting of possible disturbance inputs.

Maximal output admissible sets and reference governor are the key theoretical concepts used to calculate the DSS. The maximal output admissible set is defined as the set of all initial states that guarantee the satisfaction of the input/output constraints at any time in the future, even in the presence of unknown disturbance inputs with predefined disturbance bounds[14, 15]. If the initial state belongs to the maximal output admissible set, then for any anticipated disturbance sequence (that is within the predefined bounds), the closed-loop system always satisfies the constraints. Some disturbances can increase the possibility of safety constraint violation by pushing the system to a risky operation zone and they will be referred to as safety threatening disturbances in this paper. These disturbances may manifest through faults and failures originating within the system of interest as well as through abnormal situations occurring in upstream and downstream units. Hence, when the safety critical constraints and the safety threatening disturbances are included in the process model, the maximal admissible set becomes the DSS of the process. Since it is not possible to account for all possible disturbances in a real system, the size of the DSS could be used as a safety metric to measure the ability of the process to eliminate effects of other random disturbances.

Figure 1 below is a schematic explaining the DSS, where the dynamic response from point $\mathbf{P_1}$ in state space that lies within and point $\mathbf{P_2}$ in state space that lies outside the DSS, under a perturbed scenario.

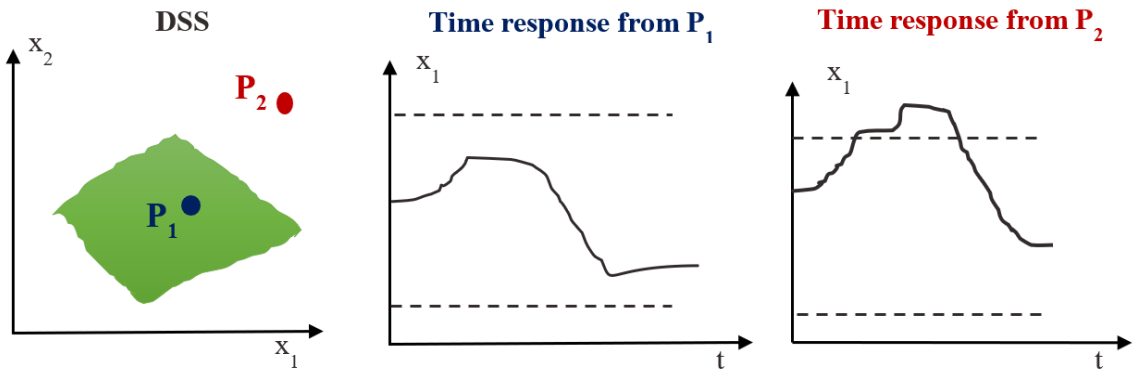


Figure 1: Illustration of the dynamic safe sets (DSS) concept

Set point changes in processes are not uncommon in industry, especially during abnormal scenarios when there may be a need for large and sudden set point changes. Control strategies must be designed to accommodate such requirements while accounting for the safety critical constraints in order to achieve maximum safety. For this purpose, the concept of reference governor [16] is used. Reference governor is a supervisory nonlinear control scheme that is added to an existing closed-loop system that attenuates the reference signal that is to be tracked, only when necessary, to avoid constraint violations and stay within the safe region. The traditional control-loop and reference governor scheme are shown in figure 2. The reference governor requires information to help predict the possibility of future constraint violation. The maximal output admissible sets will be used as the predictive tool that enables the implementation of reference governor in this work.

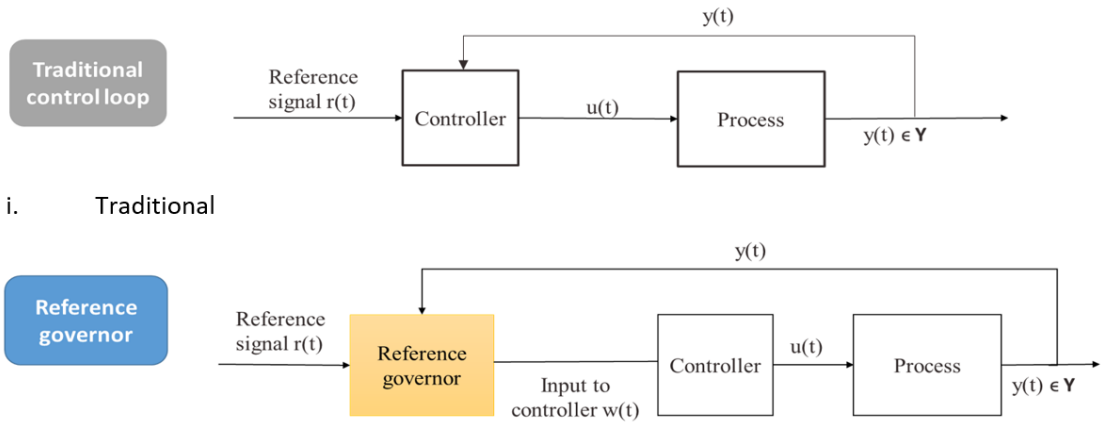


Figure 2: i. Traditional and ii. Reference governor control schemes

3 Mathematical formulation of the concept of dynamic safe set (DSS)- Dynamic safety margin (DSM)

An overview of the maximal output admissible sets for disturbance-free case and with disturbance inputs accounted for is briefly reviewed first. The concepts are based on the theory developed in [14] and [15]. It is followed by an introduction to the reference governor theory [16]. The overview of theoretical concepts will be followed by the proposed mathematical definition of dynamic safe

sets (DSS). Lastly, a quantitative methodology to evaluate the size of n-dimensional DSS is proposed via defining the dynamic safety margin (DSM).

3.1 Brief overview of pertinent systems theory concepts

3.1.1 Determination of maximal output admissible sets without disturbance inputs (based on [14]):

Consider a discrete-time linear system:

$$x(t+1) = A_P x(t) + B_P u(t) \quad (1)$$

$$y(t) = C_P x(t) + D_P u(t) \quad (2)$$

where $x \in \mathbf{R^n}$, $y \in \mathbf{R^p}$ and $u \in \mathbf{R^m}$ are the states, outputs and control inputs for the process. A_P, B_P, C_P, D_P are real matrices of appropriate dimensions.

If the control input is assumed to take the form of a linear state feedback law with $u(t) = K\,x(t)$ with K being the controller gain, then the closed-loop system can be described as below:

$$x(t+1) = A\,x(t), \text{where } A = A_P + B_P K \quad (3)$$

$$y(t) = C\,x(t), \text{where } C = C_P + D_P K \quad (4)$$

The set of output constraints that the system outputs should meet at all times is **Y,** that is,

$$y(t) = \{ Cx(t) \in \mathbf{Y} \quad \forall \quad t \in \mathbf{N^+} \} \quad (5)$$

where $\mathbf{N^+}$ is the set of positive integers. Note that the state and process input constraints can be expressed through the set **Y** as a set of inequalities in y.

The maximal output admissible set ($\mathbf{O_\infty}$) is defined as the set of all initial conditions **Z**, s.t, $x(0) \in \mathbf{Z}$ implies, $Cx(t) \in \mathbf{Y}$ is satisfied for all $t \in \mathbf{N^+}$.

That is,

$$\mathbf{O_\infty}(A, C, Y) = \{x \in \mathbf{R^n}: CA^t x \in \mathbf{Y} \quad \forall \quad t \in \mathbf{N^+}\} \quad (6)$$

The $\mathbf{O_\infty}$ is represented by a finite set of linear inequalities if and only if $\mathbf{O_t} = \mathbf{O_{t+1}}$ for some finite t where,

$$\mathbf{O_t} = \{x(0) \in \mathbf{R^n}: \quad y(k) \in \mathbf{Y} \quad \forall \quad k = 0, \ldots, t\} \quad (7)$$

The finite determination of $\mathbf{O_\infty}$ is feasible under some reasonable assumptions (see [14])

More often **Y** is defined by inequalities,

$$\mathbf{Y} = \{ y \in \mathbf{R^p} : f_i(y) \leq 0, \; i = 1, .., s\}. \quad (8)$$

For such systems, under the assumptions,

- **i.** A is Lyapunov stable,
- **ii.** the functions $f_i: \mathbf{R^n} \rightarrow \mathbf{R}$, for $i = 1, .., s$ are continuous and
- **iii.** $f_i(0) \leq 0$

and by defining $g_i: \mathbf{R^n} \rightarrow \mathbf{R}$, with

$$g_i(x) = \sup\{ f_i(CA^t x): \quad t \in \mathbf{N}^+\}, \tag{9}$$

the maximal output admissible set can be defined by,

$$\mathbf{O}_\infty = \{x \in \mathbf{R^n} : \ g_i(x) \leq 0, \ i = 1,..,s\} \tag{10}$$

See [14] for proof.

For $\mathbf{O_\infty}$ represented by eq. (10), there exists a nonempty set of integers $S^* \subset \{1, \dots, s\}$ and indexes t_i^*, $i \in S^*$, such that $t^* = \max\{ t_i^*, i \in S^*\}$. That is,

$$\mathbf{O}_\infty = \{x \in \mathbf{R^n} : \ f_i(CA^t x) \leq 0, \ i \in S^*, t \in \{0, \dots., t_i^*\}\} \tag{11}$$

Eq. (11) can also be represented by the following recursion that will be the basis for algorithms used in mathematical programming software to determine $\mathbf{O}_\infty$.

$$\mathbf{O_{t+1}} = \mathbf{O_t} \cap \{x \in \mathbf{R^n}: CA^{t+1} x \in \mathbf{Y} = f_i(CA^t x) \leq 0\}, \quad \mathbf{O_0} = \{x : Cx \in \mathbf{Y}\} \tag{12}$$

The reader can refer to [14] for conditions necessary for finite determination O_∞ and the recursive optimization algorithm for calculating O_∞.

3.1.2 Determination of maximal output admissible sets with disturbance inputs (based on [15])

The system described in the previous subsection may be subject to bounded disturbance inputs $w(t) \in \mathbf{W} \subset \mathbf{R^m}$, $t \in \mathbf{N}^+$ in addition to $y(t) \in \mathbf{Y}$, $t \in \mathbf{N}^+$. It is then represented by,

$$x(t+1) = Ax(t) + Bw(t) \tag{13}$$

$$y(t) = Cx(t) + Dw(t) \tag{14}$$

where $w(t) \in \mathbf{R^m}$ is the disturbance vector and x(t) and y(t) are same as in the previous disturbance free case. A, B, C and D are real matrices in appropriate dimension.

Then the maximal output admissible set is defined as the set of all initial conditions x(0) such that,

$$y(t) \in \mathbf{Y}, \quad \forall\, w(t) \in \mathbf{W}, \quad \forall \quad t \in \mathbf{N}^+. \tag{15}$$

That is,

$$\mathbf{O}_\infty = \{x(0) \in \mathbf{R^n} : \ y(t) \in \mathbf{Y}, \ \forall\, w(t) \in \mathbf{W}, \forall\, t \in \mathbf{N}^+\} \tag{16}$$

The output y(t) is represented by,

$$y(t) = \begin{cases} Cx(0) + Dw(0), & t = 0 \\ CA^t x(0) + \sum_{k=0}^{t-1} CA^{(t-k-1)} Bw(k) + Dw(t), & t \geq 1 \end{cases} \tag{17}$$

In order to establish the recursion necessary for the algorithmic determination of O_∞, define

$$\mathbf{O_t} = \{x(0) \in \mathbf{R^n}: y(k) \in \mathbf{Y} \ \forall\, k = 0, \dots, t \text{ and } \forall\, \mathbf{w} \in \mathbf{W}\} \tag{18}$$

Then,

$$\mathbf{O_0} = \{\phi \in \mathbf{R^n}: C\phi + D\psi \in \mathbf{Y} \ \forall\, \psi \in \mathbf{W}\} = \Gamma \tag{19}$$

$$\mathbf{O_{t+1}} = \{\phi \in \mathbf{R^n}: \ C\phi + D\psi \in \mathbf{Y}, \quad A\phi + B\psi \in \mathbf{O_t} \quad \forall\, \psi \in \mathbf{W}\}$$

$$= \{\phi \in \Gamma: \quad A\phi + B\psi \in \mathbf{O_t} \quad \forall \psi \in \mathbf{W}\}, t \in \mathbf{N^+} \tag{20}$$

The Pontryagin difference (P-subtraction) is used to represent eq. (19) and eq. (20) suitable for algorithmic procedures. P-subtraction is a set operation that can be defined for sets $\mathbf{U, V} \subset \mathbf{R^n}$ as below:

$$\mathbf{U} \sim \mathbf{V} = \{z \in \mathbf{R^n}: z + v \in \mathbf{U} \; \forall \, v \in \mathbf{V}\} \tag{21}$$

The P-subtraction is used to represent $\mathbf{O_{t+1}}$ in a compact form and thus help in the development of algorithmic procedures for determining the maximal output admissible sets.

Applying the P-difference to eq. (17),

$$\mathbf{Y_0} = \mathbf{Y} \sim D\mathbf{W}, \tag{22}$$

$$\mathbf{Y_t} = \mathbf{Y} \sim D\mathbf{W} \sim \ldots\ldots \sim CA^{(t-1)}B\mathbf{W}, t \geq 1 \tag{23}$$

Then,

$$\mathbf{O_t} = \{x(0) \in \mathbf{R^n}: \quad CA^k x(0) \in \mathbf{Y_k} \; \forall \, k = 0, \ldots, t\} \tag{24}$$

Combining eq. (22), eq. (23) and eq. (24), the recursions are established as follows:

$$\mathbf{Y_{t+1}} = \mathbf{Y_t} \sim CA^t B\mathbf{W}, \qquad \mathbf{Y_0} = \mathbf{Y} \sim D\mathbf{W} \tag{25}$$

$$\mathbf{O_{t+1}} = \mathbf{O_t} \cap \{\phi \in \mathbf{R^n}: CA^{t+1} \phi \in \mathbf{Y_{t+1}}\}, \quad \mathbf{O_0} = \{\phi : C\phi \in \mathbf{Y_0}\} \tag{26}$$

The conditions for finite determination of $\mathbf{O_\infty}$ and the optimization algorithm for calculating O_∞ in eq. (26) are given in [15].

3.1.3 Reference governor:

Reference governor is a nonlinear add-on device to an already existing closed-loop system, which attenuates the input command, when necessary. The theory on discrete-time reference governors developed in [16, 17] is adopted for implementation in this work. An overview of this concept for systems without disturbance inputs is given below.

Consider the system,

$$x(t+1) = Ax(t) + Bv(t)$$

$$y(t) = Cx(t) + Dv(t)$$

where $x(t) \in \mathbf{R^n}$ is the state vector, $v(t) \in \mathbf{R^m}$ is the reference signal vector that is to be tracked and $y(t) \in \mathbf{R^p}$ is the output vector of the closed-loop system for $t \in \mathbf{N^+}$. See figure 3 below for a schematic of the reference governor.

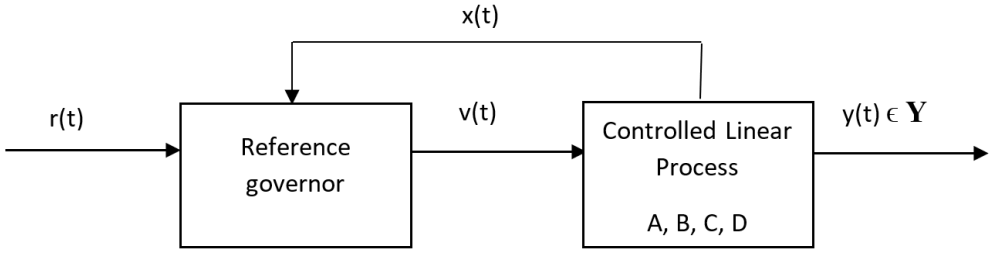


Figure 3: Schematic for reference governor

The reference governor modifies the input signal as follows,

$$v(t+1) = v(t) + K(r,x)\,(r(t) - v(t)) \text{ where } K \in [0,1],$$

$$K = \max\{k \in [0,1]: \begin{bmatrix} v & k(r-v) \\ Ax + B_v v & 0 \end{bmatrix} \in \mathbf{O}_\infty\} \quad (27)$$

This will result in the following closed-loop system:

$$x_G(t+1) = A_G x_G(t) + B_G k(r(t) - [I\ 0]x_G(t))$$

$$y_G = C_G x_G(t) \in \mathbf{Y}$$

where,

$$x_G = \begin{bmatrix} v \\ x \end{bmatrix}, A_G = \begin{bmatrix} I & 0 \\ B & A \end{bmatrix}, B_G = \begin{bmatrix} I \\ 0 \end{bmatrix}, C_G = [\,D \quad C\,]$$

$$K = \max\{k \in [0,1]: x(t+1) \in \mathbf{O}_\infty\,(A_G, B_G, \mathbf{Y})\} \quad (28)$$

The maximal output admissible set will be calculated for the system in eq. (29) by setting K as 0 initially. The algorithm for implementing reference governor for systems with disturbance inputs are provided in [18]. The optimization algorithm required for real time implementation is also provided in [18].

Although these concepts have existed in literature for more than 2 decades, its application has been mostly limited to aerospace and electrical engineering [19-23]. In chemical engineering literature, the use of maximal output admissible sets is limited to stability proofs in MPC schemes [10, 24, 25]. In this paper, we aim to exploit its capability in designing safer control systems for chemical processes.

3.2 Definition of the Dynamic Safe Set (DSS)

The concepts introduced above are used to mathematically define the dynamic safe sets. The definition of maximal output admissible set in eq. (16) shows that the output y(t) is forced to lie within the constraint set **Y** at all times. Typically, the safety critical constraints are derived from imposing bounds on linear combinations of state and output variables like the onset temperature of a runaway reaction, the maximum allowable working pressure of a vessel and the limits on controller actuator. These inequalities can be incorporated through the set **Y** such that the maximal output admissible set guarantees the satisfaction of safety critical constraints. The trajectory of output y(t) defined in eq. (17) considers also the possibility of disturbances w(t) in the process. This allows for designing systems that respect the constraints, accounting for system dynamics even in the presence of unknown disturbances.

Furthermore, there can be several possible disturbances and random noises that can push the system away from the steady-state, which the control system is generally capable of handling. In addition to these, there could be unusually large and sudden persistent disturbances occurring during abnormal situations of plant operation. Such disturbances can have severe impact on the dynamics of the process. These adverse disturbances that threaten the integrity of the process are referred to as the safety threatening disturbances in this paper. It is important that for safe operation of the process, the effects of these disturbances on the process dynamics must be included in the control system design. The set **W** in eq. (16) can include the ranges of safety threatening disturbances that are defined through linear inequalities, with only little information known about

the anticipated disturbances. Thus, from the definition of maximal output admissible sets, the set **W** inherently accounts for any possible disturbance sequence w(t), including sudden or erratic ones, by forcing y(t) to satisfy the output constraints **Y** for any w(t) in **W**.

Hence, when the system in eq. (16) has the safety critical constraints (**Y**) and the potential safety threatening disturbance ranges (set **W**) accounted for, the maximal output admissible sets become the dynamic safe sets. The dynamic safe set is the collection of all initial states that guarantee the enforcement of the safety critical constraints while respecting the process dynamics even in the presence of adverse safety threatening disturbance sequences. When the DSS is large, the process has the capability to eliminate the effect of disturbances even when the process state is initially perturbed due to unknown reasons. Some causes of these perturbations can be model uncertainties, inaccuracies in measurement sensors and equipment failures and faults. Hence, it is possible to enhance safety by increasing the size of the DSS by choosing the design parameters accordingly. The challenge however is to identify a meaningful DSS quantification methodology that can be useful for interpreting the DSS of higher order systems.

3.3 Definition of the dynamic safety margin (DSM)

It is necessary to develop a method to extract physically meaningful information from the n-dimensional DSS that is relevant and aids in safer design. For this purpose, a concept of dynamic safety margin (DSM) is proposed in this paper. It is defined as the minimum distance of the steady state operating point from the boundary of the DSS that is represented by a set of linear inequality constraints. The dynamic safety margin can be viewed as the maximum radius of a ball in the n-dimensional state space centered at the steady state that lies within the DSS.

Of course, to be able to define a norm in the presence of different units of the state variables, appropriate normalization will be necessary. Normalization of the state variables with respect to the potential consequences associated with their deviation from the steady state value seems reasonable since the ultimate design objective is to maximize safety. The potential to cause harm, in other words, the hazard associated with the magnitude of deviation is different for different state variables. The difference in increased threat is leveraged to define the scale factor (σ) for each state variable. It is the ratio of change in a state variable (x_i) to change in a reference state variable (x_r) that produces the same effect on the hazard evaluated.

That is,

$$\sigma_i = \frac{\Delta x_i}{\Delta x_r} \tag{29}$$

The scale factors for the states are used to transform the DSS from the original state coordinates to the transformed coordinates $\bar{x} = \Sigma x$, where the transformation matrix Σ is given by,

$$\Sigma = \begin{bmatrix} \sigma_i & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \sigma_n \end{bmatrix},$$

Assume the DSS in the original state space calculated around the steady state x_S is defined by the set of inequalities,

$$\boldsymbol{\Phi} = \{ \phi_j(x) = a_j^T x - c_j \leq 0, j = 1, \dots . q\}$$

Then, the set of inequalities defining the DSS in the transformed state space is,

$$\phi_j(\bar{x}) = \bar{a}_j^T \bar{x} - c_j \leq 0,\ j = 1, \dots . q \text{ , where } \bar{a}_j^T = (a_j^T \Sigma^{-1})$$

Using the projection theorem from linear algebra, the minimum distance of the steady-state $\bar{x}_S$ from each of the boundary equation $(\phi_j(\bar{x}) = 0)$ can be given by,

$$d_j = \text{abs}\left(\frac{\left(c_j - \bar{a}_j^T . \bar{x}_S\right)}{||\bar{a}_j||_2}\right), \quad j = \{1, 2, \ldots . q\} .$$

The dynamic safety margin (DSM) is then defined as,

$$\text{DSM} = \min_j d_j, \quad j = \{1, 2, \ldots . q\}. \tag{30}$$

The safety margin of states can be represented in units of the reference variable or the individual state variable by dividing the DSM by the respective σ_i. This is a measure of the minimum tolerable deviation of the state variable from its steady state value. The DSM depends on the ranges of safety threatening disturbances along with the other design parameters. It could be a conservative measure of the process safety performance, especially when adverse scenarios representing abnormal situations are included in the disturbance set **W**. An example application of the individual state margins is to design the process such that the margins of each state are at least as large as the accuracy of their measurement sensors.

An approach to address the process control design problem based on the proposed DSS and DSM concepts are outlined in the next section.

4 Proposed DSS based approach for process control design

The key ideas identified in the control system design with maximal safety, that form the basis of the proposed approach, are now outlined. Firstly, the controller set point that sets the steady state of operation of the process can play a role in system safeness. Secondly, the actuator characteristics and the control strategy and their parameters can significantly affect the system dynamics in presence of disturbances and set point changes. Thirdly, in the event of abnormal situations that may be accompanied by large and sudden changes in operating conditions, it is of utmost importance that the control system is capable of handling them while satisfying the safety critical constraints.

The proposed approach is devised based on the understanding that DSS reasonably characterizes the safeness of the process, by accounting for safety constraints and dynamic effects of safety threatening disturbances. It then leads to the conceptual idea that the DSS along with the DSM can be used as a guide in addressing the ideas stated above. It is assumed that a process model to capture the dynamics is available and that the safety critical constraints are identified based on a thorough understanding of the process. It is also reasonable to account for disturbance inputs that represent possible abnormal situations in the DSS calculation.

Typically, the control system is designed with objective to eliminate the effects of disturbances quickly and safely around a set point. Of course, it is assumed that potential set points considered maintain certain essential performance metrics with respect to other design criteria. The favorable set points can then be chosen based on the DSS and DSM they offer under some nominal controller and actuator design. Once the relatively safer steady states are identified, the control system can be designed, that includes the actuator system and the selection of strategy and parameters. A grid of design parameters that consist of possible control laws, actuator design parameters and controller tuning parameters can be used to generate a set of closed-loop systems, operating at each

of the identified safe set points. The DSS and DSM calculations can be performed for these closed-loop systems.

The approach will provide designs that represent maximal safeness. When there are multiple designs that offer reasonable safeness, the controller performance requirements can be used as additional performance metrics. Financial considerations involved in the actuator system design can also be used as metrics to identify the final design.

In the event of an abnormal situation, there may be a need for a large and sudden set point change. Because controllers that are normally used for disturbance rejection are tuned to be aggressive (with large controller gains), when there is a sudden need for a set point change, special care should be taken for safe transition. The use of reference governor scheme is proposed as an addon scheme to guide the system and help prevent potential actuator saturation.

It will be seen from the case study that follows that the proposed approach captures multiple facets of safety considerations. The final design configuration will provide maximal safeness and reasonable performance with respect to other criteria. The time responses of the closed-loop system for the final design configuration along with the reference governor scheme will indicate the effectiveness of the design approach.

5 Case Study

5.1 Case study description

The DSS approach for safety-centered design and control was tested on a continuous-stirred-tank-reactor (CSTR) handling an exothermic reaction. T2 Laboratories manufactured methylcyclopentadienyl manganese tricarbonyl in a 2500-gallon batch reactor. In 2007, an explosion occurred at the plant during the production process resulting in 4 fatalities and several injuries. The incident took place when there was insufficient cooling provided to the reactor and the temperature increased uncontrollably causing reactor rupture. Hydrogen and other flammable chemicals were ignited resulting in a massive explosion. In this paper, the reactions of T2 Laboratories that led to the explosion are modeled in a CSTR reactor (as shown in Figure 4), instead of the batch reactor originally used at T2.

The feed streams reactant methylcyclopentadiene (A) in solvent diglyme (S) and liquid sodium (B), are both heated in a preheater before being fed to the reactor. The reactor temperature control loop maintains the reactor temperature at the required set-point. The temperature of the reactor (T) is the controlled variable, the cooling system heat transfer coefficient (U) is the manipulated variable (control input) and the fluctuations in reactor inlet feed temperature (T_0) is accounted for as potential disturbance source in the model. The heat transfer coefficient is manipulated by adjusting the flowrate of the cooling water based on correlations available from literature. For the sake of simplicity, U will be treated as the manipulated input for this case study.

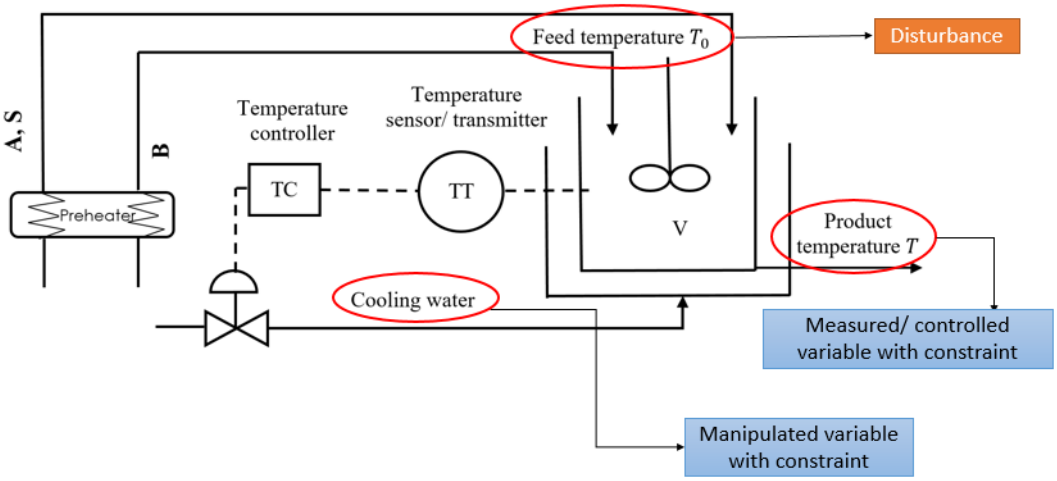


Figure 4: Process flow diagram of the modified T2 Laboratories process in a CSTR

The reactions considered for study can be modelled as follows:

$$\text{Reaction 1:} \quad A + B \xrightarrow{k_1} C + \tfrac{1}{2} D$$

$$\text{Reaction 2:} \quad S \xrightarrow{k_2} 3D + \text{byproducts}$$

In particular,

$$\underset{\mathbf{A}}{\text{Methylcyclopentadiene}} + \underset{\mathbf{B}}{\text{Sodium}} \xrightarrow[\mathbf{S}]{\text{Diglyme}} \underset{\mathbf{C}}{\text{Sodium Methylcyclopentadiene}} + \underset{\mathbf{D}}{\text{Hydrogen}}$$

$$\underset{\mathbf{S}}{\text{Diglyme}} \xrightarrow{\text{Sodium}} \underset{\mathbf{D}}{\text{Hydrogen}} + \text{byproducts}$$

The mass and energy balances for the reactor are presented below:

$$\frac{dC_A}{dt} = r_{1A} + v_0 * \frac{(C_{A0} - C_A)}{V}$$

$$\frac{dT}{dt} = \frac{V*(r_{1A}\Delta H_{r1A} + r_{2S}\Delta H_{r2S}) - (U_S + U)*A_x*(T - 373)}{\Sigma NC_p}) + v_0 * \frac{(T_0 - T)}{V}$$

where C_A is the concentration of the reactant methylcyclopentadiene, T is the temperature of the reactor, v_0 is the volumetric flowrate of the feed and V is the reactor volume, U_S is the steady state heat transfer coefficient, ΣNC_p is the heat capacity of the system, A_x is the heat transfer area of the exchanger, r_{1A} and r_{2S} are the reaction rates for reactions 1 and 2 respectively, ΔH_{r1A} and ΔH_{r2S} are the heat of reactions for reactions 1 and 2 respectively.

The closed-loop processes under proportinal (P) and proportional-integral (PI) contol strategies can be respresented by,

P-Controller: $U = k_{c*}(T_S - T)$ and

PI-Controller: $U = k_c * (T_S - T) + \frac{I}{\tau_i}$ along with the ode $\frac{dI}{dt} = T_S - T$ to account for the integral of error calculation,

where k_c and τ_i are the controller parameters, gain and integral time respectively.

Reaction 2 is a side reaction that has a negligible rate when operated at temperatures less than 460 K. However, upon reaching 480 K the rate of side reaction becomes significant as it has an activation energy of more than 6 times that of the desired main reaction. This will cause an uncontrolled increase in reaction rate at higher temperatures. As both reactions produce hydrogen gas, there is a possibility of steep increase in the pressure that can cause a reactor wall rupture. Based on these observations, the following temperature constraint will be imposed.

$T < 480$ K

The maximum available manipulated input (U_{max}), which is a design parameter, will be included as a safety critical constraint. The reason here is that a sustained violation of this constraint may lead to divergence of the deviation in reactor temperature, which may result in a runaway scenario.

$U < U_{max}$

It is anticipated that upstream units and preheater malfunction may bring in fluctuations in the reactor feed temperature. The range of the reactor feed temperature (T_0) is expected to be between 405 K and 430 K. The upper limit was intentionally chosen to be an unusually large value to account for rare events which can more than likely push the system to hazardous operation zone. Hence, T_0 is included as a safety threatening disturbance.

$405 < T_0 < 430$ K

Based on the system description provided, the design parameters that are to be chosen are (i). the maximum heat transfer coefficient (U_{max}) and (ii). the controller parameters (k_c for P-Controller, k_c and τ_i for PI-controller). This system can be viewed as a representative example for exothermic reactors with cooling and temperature control system.

The above nonlinear dynamic model is linearized and discretized around different operating conditions that are to be investigated, as shown in eq. (13) and eq. (14) of section 3:

$$x_d(k+1) = A_d x_d(k) + B_d w(k),$$

$$y_d(k) = C_d x_d(k) + D_d w(k),$$

where the states $x_d = [C_A; T]$, output $y_d = [T; U]$,

$w \in \mathbf{W} = \{ 405 \leq w = T_0 \leq 430\}$ and

$$y_d \in \mathbf{Y} = \{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} y_d \leq \begin{matrix} 480 \\ U_{max} \end{matrix} \}$$

Selection of scale factor for normalizing the states required for determining the DSM

For this case study, the increase in reaction rate is chosen as the common hazard used to define the scaling factor (SF) for normalizing the states (discussed in section 3). If temperature is chosen as the reference state variable, the scale factor of concentration becomes the ratio of change in

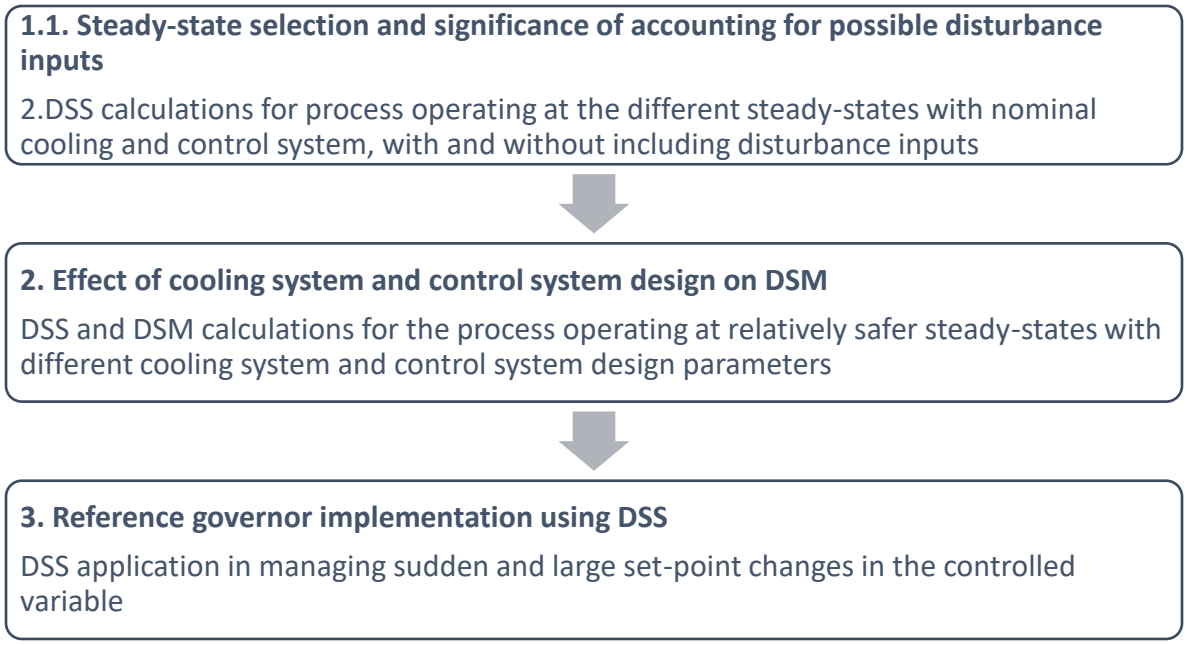
concentration to change in temperature that brings similar effect on change in reaction rate. The SF for temperature is 1 based on the definition. The SF for the state variables will depend on the steady state operating conditions. For the operating conditions between 440 and 465 K, a value of 80 is chosen as the SF for concentration.

$$\sigma = \begin{bmatrix} 80 \ {}^{\mathrm{K}}/_{\mathrm{mol}/l} \\ 1 \end{bmatrix} \tag{31}$$

This is used to calculate the DSM around the steady state in the normalized DSS. The DSM is expressed in temperature units in the discussions that follow.

5.2 Application of the DSS approach

The approached proposed in section 4 for control system design are tested on this CSTR. This case study can be viewed as a representative example for exothermic reactors with cooling system and control system design. The results from the investigation are organized as follows:



5.2.1 Steady state selection and significance of accounting for possible disturbance inputs

The steady state ranges that are investigated are chosen to guarantee a minimum reactant conversion of 85% as the design basis. This led to selecting set point temperatures (T_S) greater than 440 K. The upper limit of the temperature range was fixed as 465 K to provide a minimum of 15 K margin with respect to the temperature constraint (T < 480 K). At these operating temperatures, the steady state heat transfer coefficient required varies between 5 and 48 kJ/K/m^2/hr. For the steady states identified for analysis, the DSS is calculated for the closed-loop system operating with nominal cooling system and control system design.

The maximum heat transfer coefficient (U_{max}) is the cooling system design parameter that is manipulated by adjusting the cooling water flowrate typically. In this case study, U_{max} is treated as an independent design parameter for illustrating the DSS and DSM concepts. Nominal values of cooling system (U_{max}) chosen are 55 and 70 kJ/m^2/K/hr so that they provide a minimum of 10

% and 38 % control input margin respectively, for all the steady states evaluated. The nominal control system chosen is a P-only controller, which is commonly used for temperature control in industry. The controller gain (k_c) of -25 is selected.

The DSS is determined for both disturbance-free case and with disturbance case to compare and understand the safety relevant information that is lost by not accounting for disturbance effects in steady state selection. The DSS for closed-loop system with nominal cooling and control system, without accounting for the disturbance inputs are shown in Figure 5 and Figure 7 respectively. For the same process, disturbance inputs were included and the results are shown in Figure 6 and Figure 8.

The results for U_{max} of 55 show that at steady states 450 and 455 K, the DSS is reduced to null sets once disturbance input was included. Accounting for disturbance input with U_{max} of 70 resulted in relatively smaller DSS (Figure 8) when compared to Figure 7 for all steady states. The results show a strong effect of choice of steady state and heat exchanger design on the size of dynamic safety. However, there are some steady states, namely, 460 and 465 K, that seem more favorable relative to the others, irrespective of the heat exchanger design. These will be taken in to account in the discussions to follow.

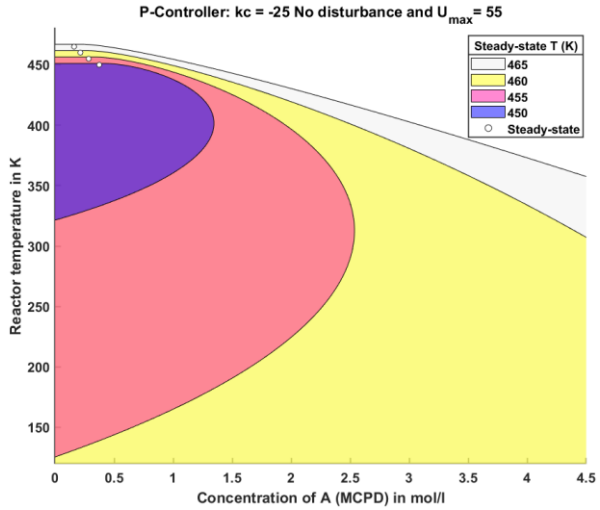


Figure 5: The DSS for P-Controller with k_c -25 and U_{max} 55. Disturbance not included.

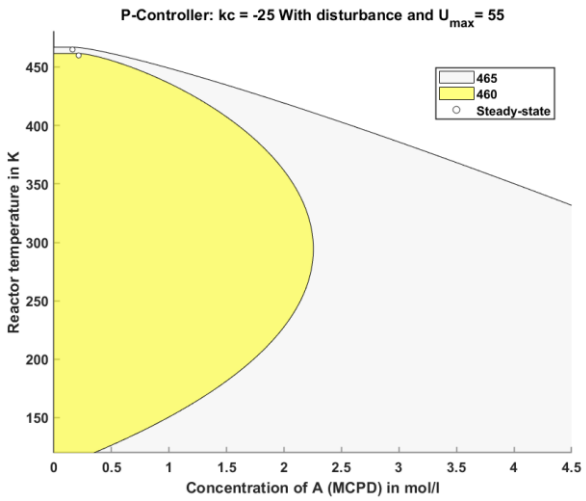


Figure 6: The DSS for P-Controller with k_c -25 and U_{max} 55. Disturbance included.

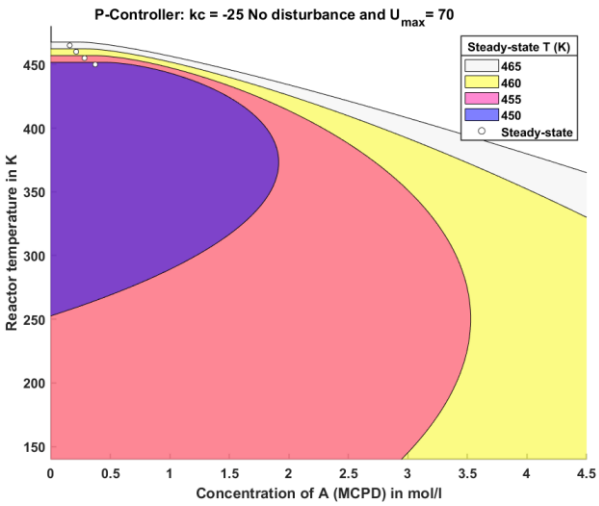


Figure 7: The DSS for P-Controller with k_c -25 and U_{max} 70. Disturbance not included.

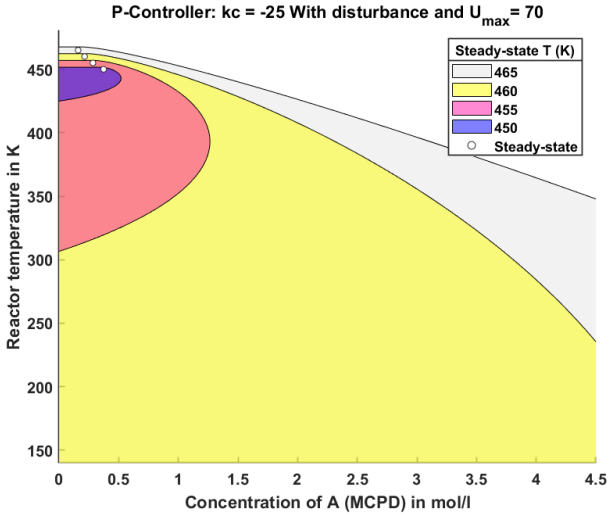
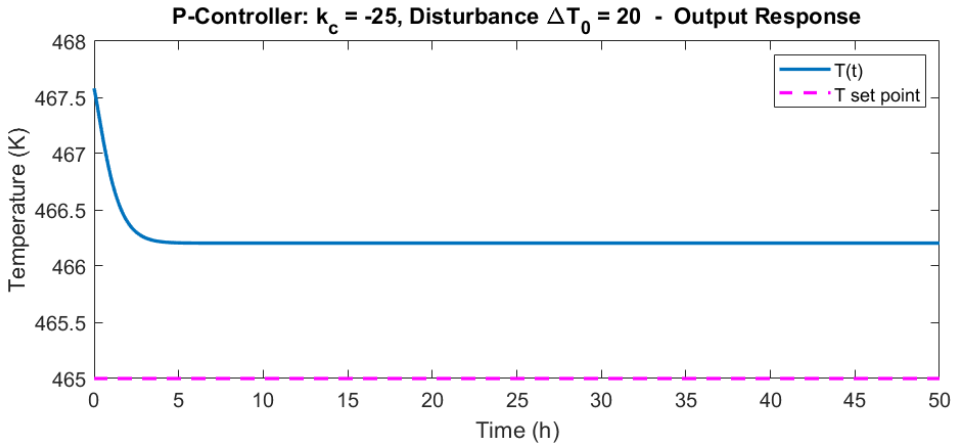
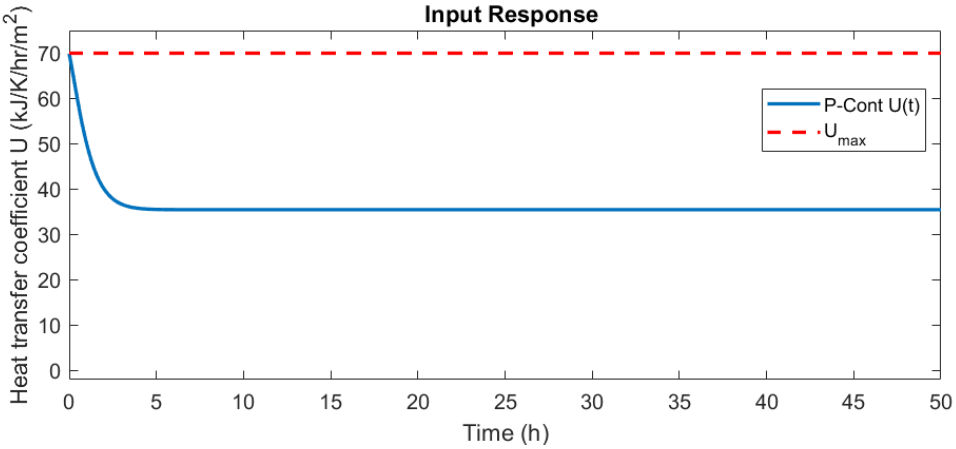


Figure 8: The DSS for P-Controller with k_c -25 and U_{max} 70. Disturbance included.

To understand the implications of the DSS better, the time responses for a system operating at 465 K with a U_{max} of 70 kJ/m^2/K/hr and an initial impulsive disturbance that results in a 2.58 K shift in reactor temperature are shown below. In addition to this, a persistent step disturbance of 20 K in T_0 is induced to the system to illustrate the most adverse conditions the system can tolerate. Figure 9 shows the output and input responses simulated for the nonlinear closed-loop system based on a P only controller with k_c -25 that was simulated in MATLAB.



(i). Output response



(ii). Input response

Figure 9: (i). Output response and (ii). Input response of the system operating at 465 K, U_{max} 70 kJ/m^2/K/hr based on a P Controller with k_c -25, under initial impulsive disturbance that shifts T by 2.58 K and step disturbance of 20 K in T_0

Although the DSS are calculated for linearized and discretized systems, these simulations show that they are adequate for designing the nonlinear process. From the results shown in figures 5 - 8, it is seen that the size of DSS tends to increase with increasing steady state temperature for a particular heat exchanger design (U_{max}). The reason for this is that with decreasing steady state temperature (T_s), the steady state cooling requirement (U_s) increases. This results in a decrease in the difference between U_{max} and U_s as T_s decreases. As a result, the excess manipulated input available for eliminating the effect of disturbances decreases. Another important observation is that, accounting for disturbances provides insights that are normally ignored while approaching the design and control problem. For this case study, the proposed DSS approach led to identifying operating steady-states 460 and 465 K as more favorable choices as they can sustain the effect of the large persistent disturbances and provide a reasonable DSS area. Analysis to further investigate the effect of other design parameters will be carried out in the next subsection.

5.2.2 Effect of cooling and control system design on DSM

P-only Controller

A grid of different heat exchanger and control system design parameters are selected for analysis in this subsection. The effect of heat exchanger design parameter was partly seen in subsection 5.2.1. The controller tuning parameters are critical design parameters as they have a direct effect on the process performance and safeness of the plant. More aggressive controllers may provide good responses but may significantly reduce the size of DSS. Firstly, the DSS was evaluated for P- controller based closed-loop system with different gains (k_c) with a fixed U_{max}. The DSM was calculated for these systems based on eq. (30) for the scale factor identified in eq. (31). It is the measure of margin of safety (or the safety buffer) around that steady state that lies within the DSS. The DSM is reported in units of the reactor temperature (K). i.e, the minimum tolerable initial deviations in the reference state variable T and the scaled state variable C_A, from their steady state values. Table 1 and Figure 10, shows the DSM with U_{max} of 70 kJ/m^2/K/hr for P-controller based closed-loop system with gains of -25, -55 and -75, while accounting for the disturbance input.

The DSM is 0.5 K for the process operating at 450 K with controller gain k_c of -75. This means, there are high chances of violation of safety critical constraints, if the reactor temperature is off by as little as 0.5 K from the steady state temperature. The results in Table 1 show that the range of DSM lies between 0.5 to 2.6 K. Although the safety margin seems to be low, it is important to note that DSM is a conservative measure of safety especially when it accounts for deliberately large disturbances. It is understood that if the ranges of disturbances accounted for are narrower, the size of the safety margin could increase and possibly allow more feasible operating steady states without null sets.

Table 1: DSM for P-only Controller with [k_c]= {-25, -55, -75} and U_{max} of 70 kJ/m^2/K/hr, after accounting for disturbance input

	DSM for process with U_{max} of 70 (scale factor 80) in K		
Steady state reactor temperature T (K)	**P-Controller k_c**		
	-25	**-55**	**-75**
465	2.6	1.2	0.9
460	2.3	1.0	0.8
455	2.0	0.9	0.7
450	1.5	0.7	0.5

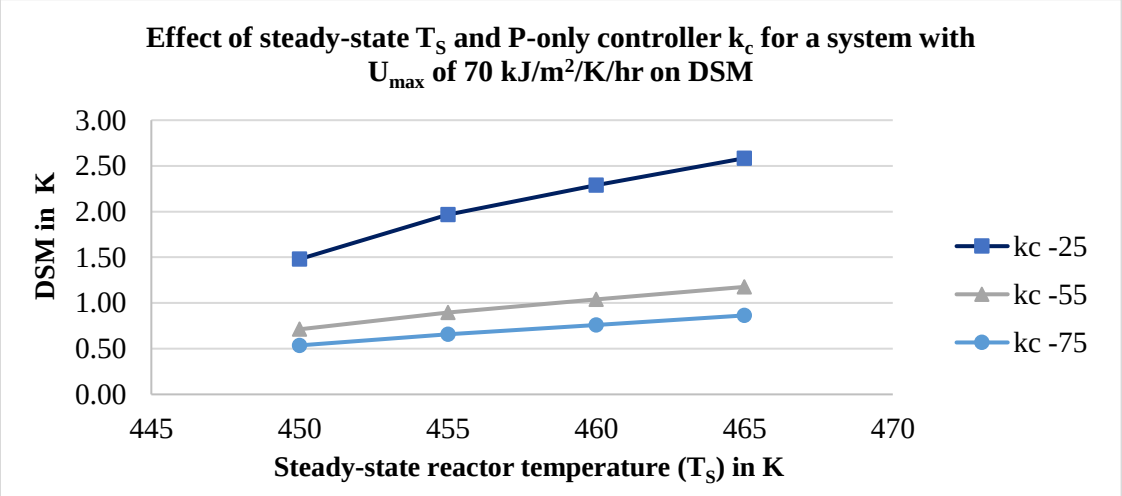
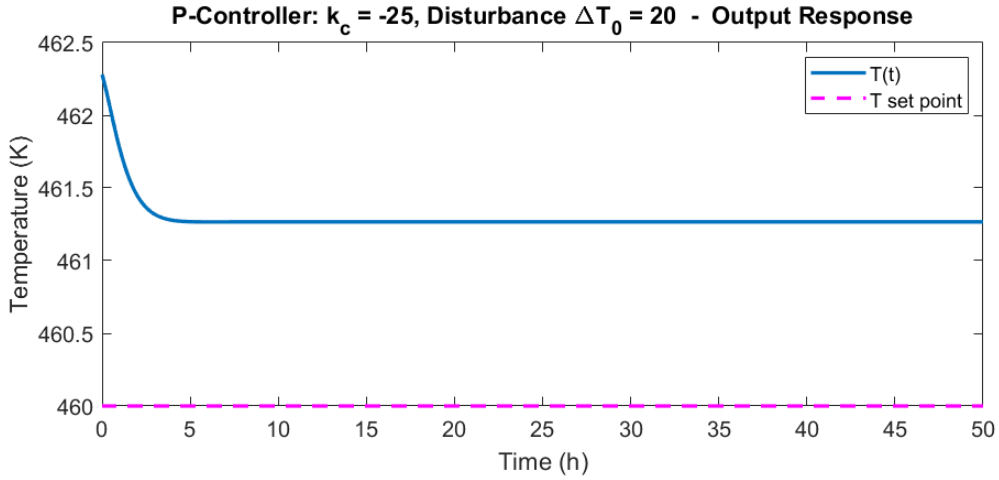
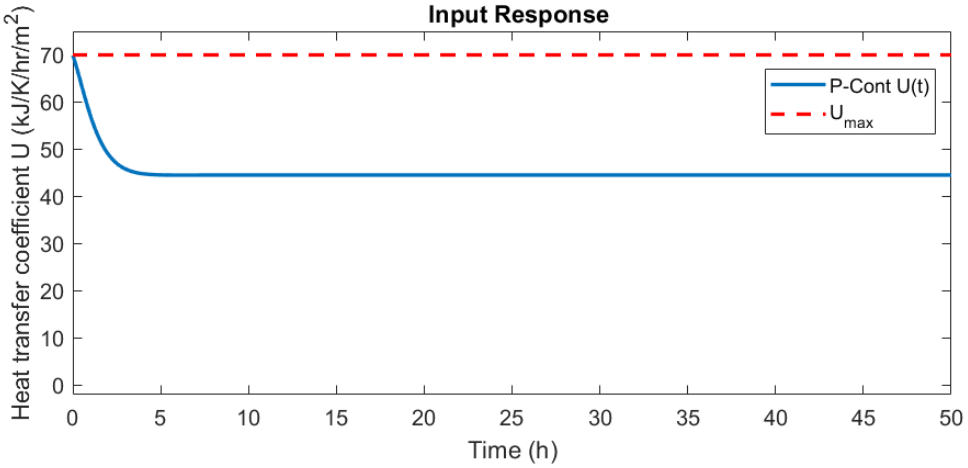


Figure 10: DSM (K) for closed-loop system with U_{max} 70 kJ/m^2/K/hr, effect of steady state temperature T_S = {450, 455, 460, 465} and P-Cont. gain k_c={-25, -55 and -75} on DSM

The time responses of the P-control based closed-loop system operating at 460 K with a gain k_c of -25 and U_{max} of 70 are shown below. From Figure 10, it is seen that the DSM is 2.28 K, that is the control system and process design can eliminate the effect of a step disturbance of 20 K in T_0, even if the reactor temperature (T) is initially perturbed by 2.28 K by an impulsive disturbance. See Figure 11 for output response and input response for the non-linear process model. The control input and the reactor temperature constraints are not violated and the effect of the disturbances in T_0 and T are both contained. There is an offset in the output variable since a P-only controller is used and the reactor reaches a new steady-steady of ~461.3 K. Increasing the absolute value of the controller gain can help reduce this offset. However, the DSM will decrease as seen in Table 1. Figure 12 show the dynamic responses of the process operating at similar conditions but with a gain k_c of -75 under an impulsive disturbance in reactor temperature that shifts it by 0.76 K and a persistent step disturbance of 20 K in T_0. The offset in the reactor temperature is decreased to 0.4 K. However, the system may violate the safety constraints for initial disturbances greater than 0.76 K.

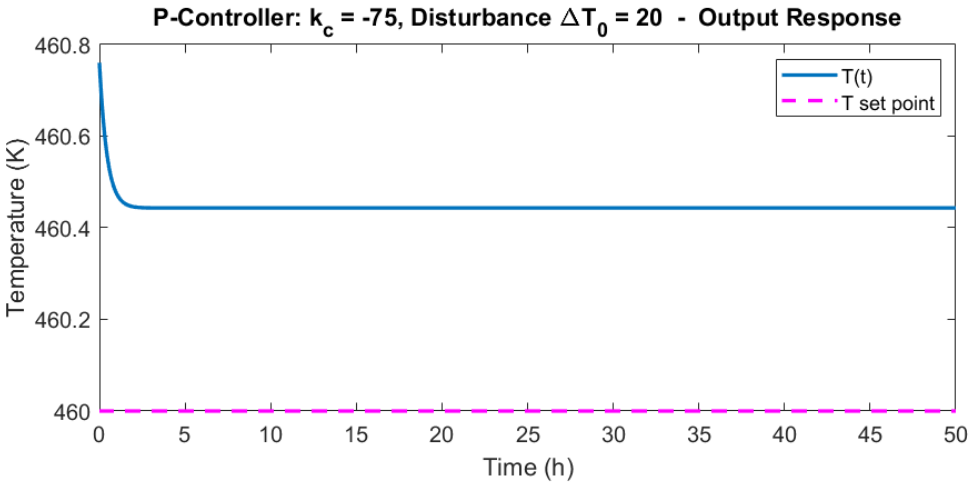


(i). Output response

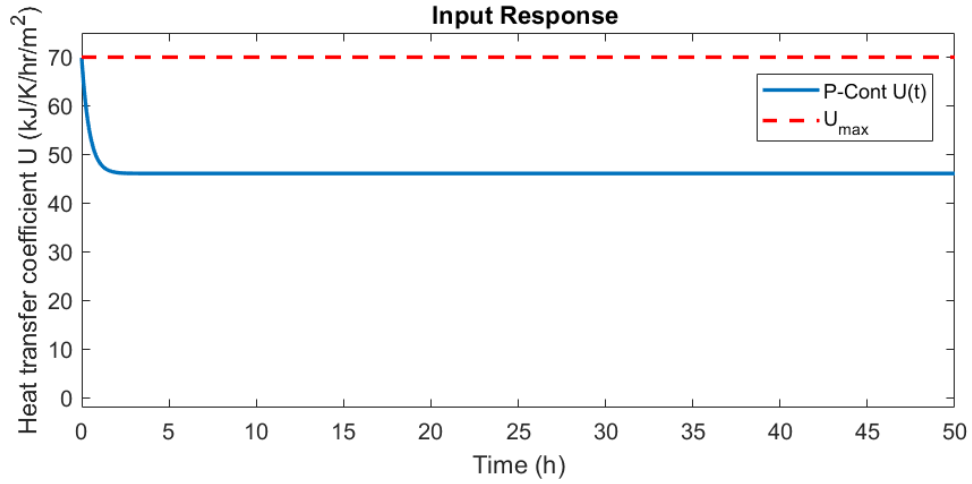


(ii). Input response

Figure 11: (i). Output response T(t) and (ii). Input U(t) response to a +20 K step disturbance in T_0 and an initial impulsive disturbance that shifts T by 2.28 K for a P-controller based closed-loop system with k_c of -25, operating at 460 K.



(i). Output response



(ii). Input response

Figure 12: (i). Output response T(t) and Input response U(t) to a +20 K step disturbance in T_0 and an initial impulsive disturbance that shifts T by 0.76 K for a P-controller based closed-loop system with k_c of -75, operating at 460 K.

P and PI Controller

The effect of U_{max} on the DSM will be investigated for the favorable steady states of 460 and 465K. Subsequently, the effect of control strategy and controller parameters will also be simultaneously studied. See figures 13-18 for the DSS calculated for different heat exchanger design parameter (U_{max}) and closed-loop system based on P and PI control strategies with gain of -25. These results demonstrate the significant role played by the integral time in determining the size of the DSS irrespective of the U_{max}. For example, the DSS is reduced to null set for a system operating at 460 K with U_{max} of 55 under the PI controller with integral time of 2 in Figure 14. In all cases, it is seen that the PI controller with an integral time of 2 significantly reduces the range of temperature (T) and concentration (C_A) that lies within the DSS when compared to the respective P-only controller based closed-loop systems.

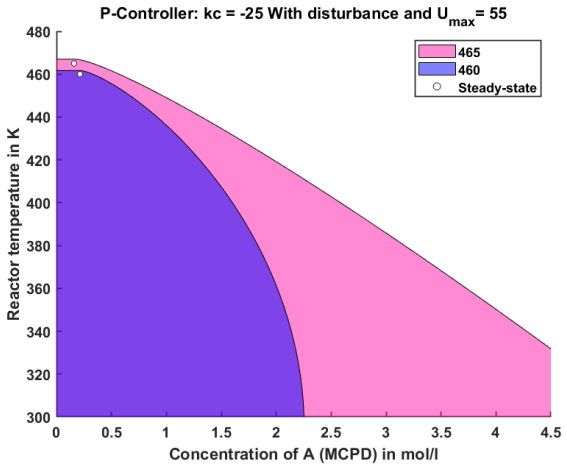


Figure 13: The DSS for P-Controller with k_c -25 and U_{max} 55 with disturbance input included

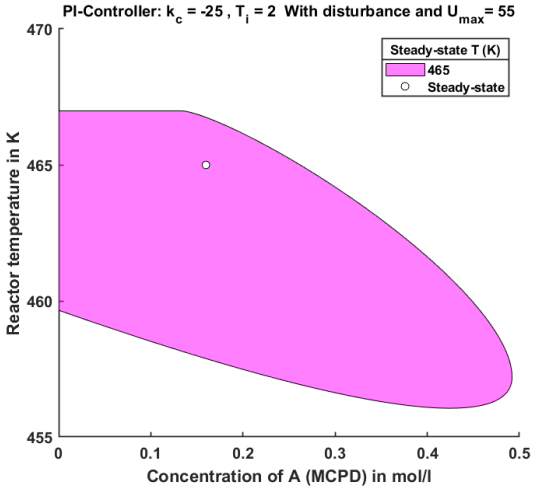


Figure 14: The DSS for PI-Controller with k_c -25 and τ_i 2 and U_{max} 55 with disturbance input included

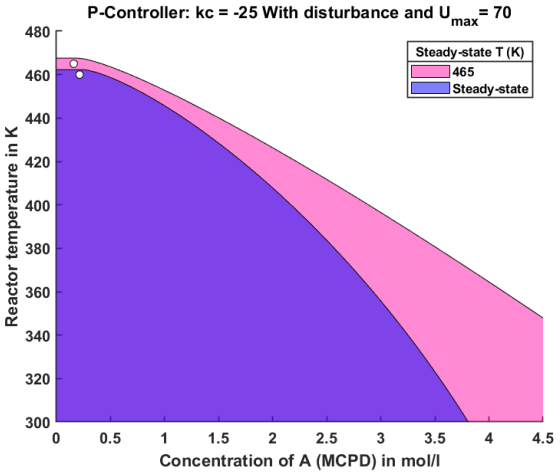


Figure 15: The DSS for P-Controller with k_c -25 and U_{max} 70 with disturbance input included

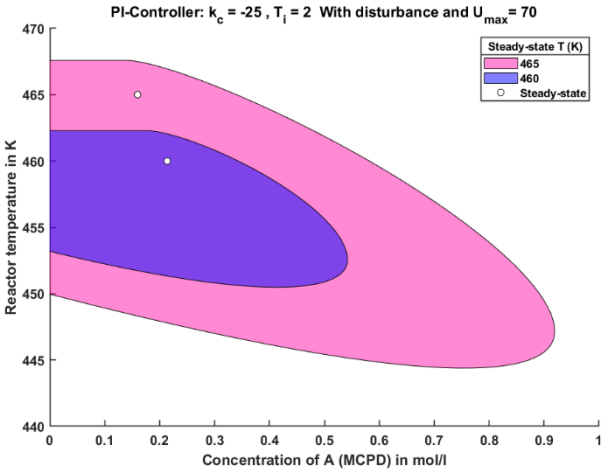


Figure 16: The DSS for PI-Controller with k_c -25 and τ_i 2 and U_{max} 70 with disturbance input included

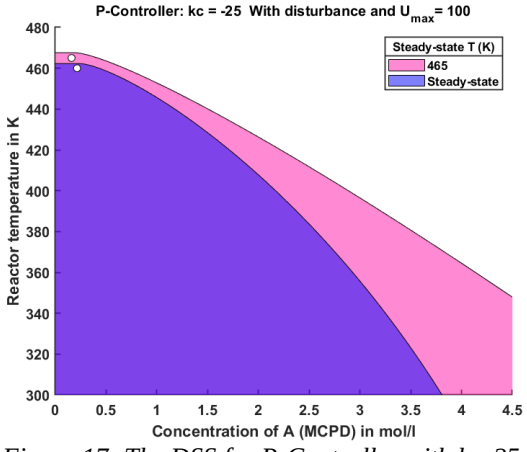


Figure 17: The DSS for P-Controller with k_c -25 and U_{max} 100 with disturbance input included

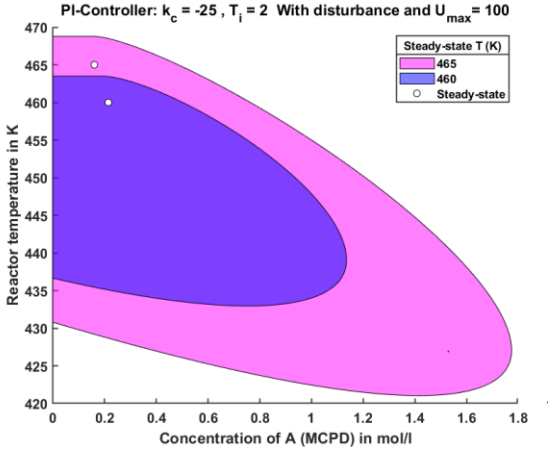


Figure 18: The DSS for PI-Controller with k_c -25 and τ_i 2 and U_{max} 100 with disturbance input included

Figure 19 shows the DSM in units of reactor temperature for different heat exchanger design parameter U_{max} (55, 70 and 100 kJ/m^2/K/hr). The results for both P and PI controller strategies

with k_c of –25 and τ_i of 0.75 and 2 are shown to compare the effect of integral time and U_{max} on DSM for the system operated at set points 460 and 465 K. The key observations are as follows:

- As expected, the DSM increases with increasing U_{max} and τ_i.
- U_{max} of 100 kJ/m^2/K/hr provides a maximum DSM of 3.8 K when a PI controller with integral time of 2 is used for the closed-loop design when operating at steady state 465 K.
- U_{max} of 55 kJ/m^2/K/hr provides a DSM of up to 1.7 K for a P only controller and reduces the DSS to null set for PI control with integral times of 2 and 0.75 when operating at 460 K.

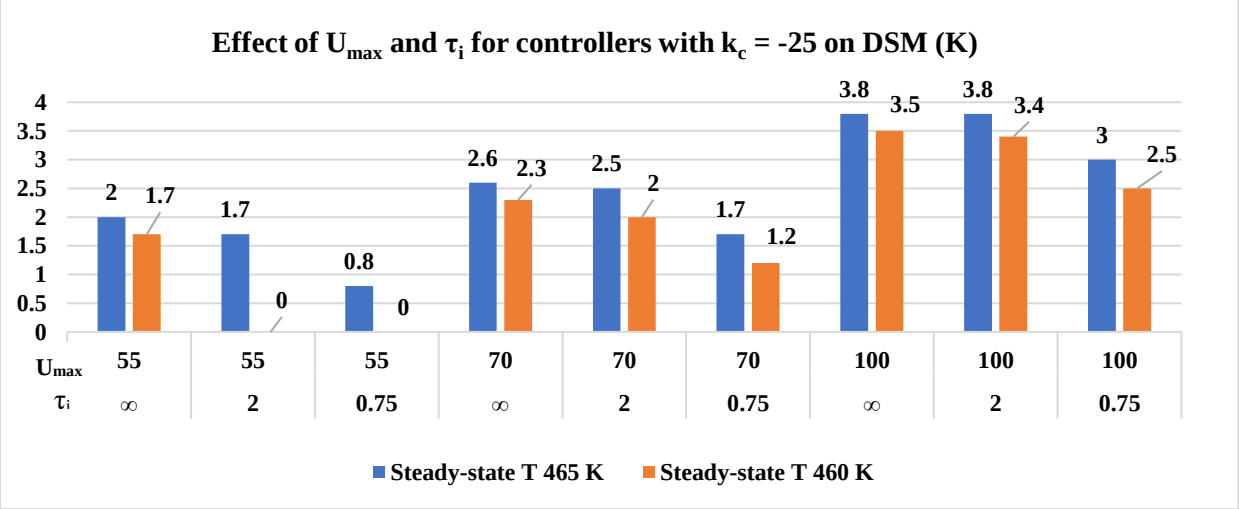


Figure 19: The DSM in units of reactor temperature (K) for [U_{max}] ={55, 70, 100}, with disturbance input included for P and PI Controllers with k_c = -25 and [τ_i]= {∞,2, 0.75}

Figure 20 shows the DSM for different controller gains and integral times for a fixed U_{max} when operated at 460 and 465 K steady states. Although, lower negative k_c and higher τ_i favors larger DSM, it is accompanied by a compromise in controller performance. That is, high negative gains can decrease the offset when using a P controller and provide faster response with zero offset when using a PI controller. The lower the integral time, the faster will be the elimination of the disturbance effects. However, very low integral times will result in unfavorable oscillatory behavior. The times responses for system with 0.75 integral time, shows such oscillatory behavior for the system operating at 460 K under a persistent disturbance of 20 K in T_0 as well as an initial impulsive disturbance of 2.5 K in T in Figure 21. Figure 22 shows the effect of using a PI controller with a higher integral time τ_i of 5 for the same disturbances, with no oscillatory behavior.

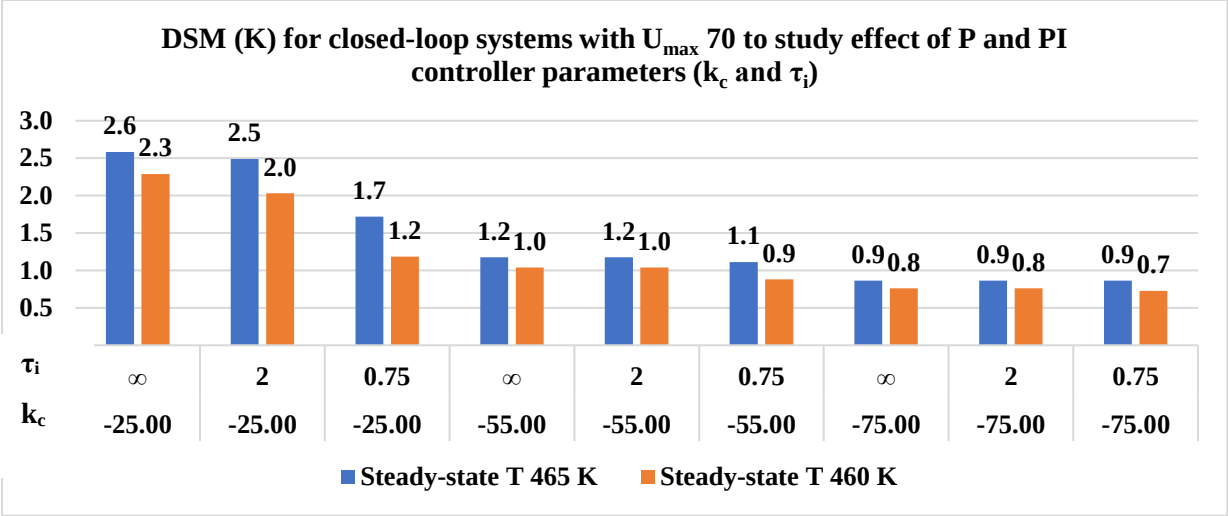
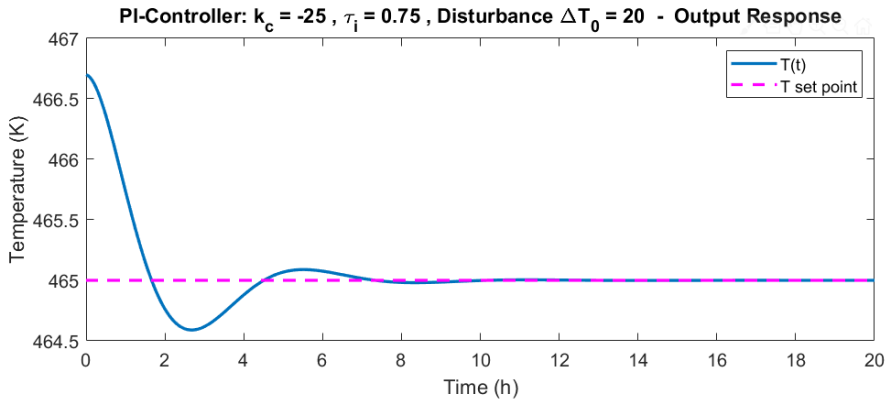
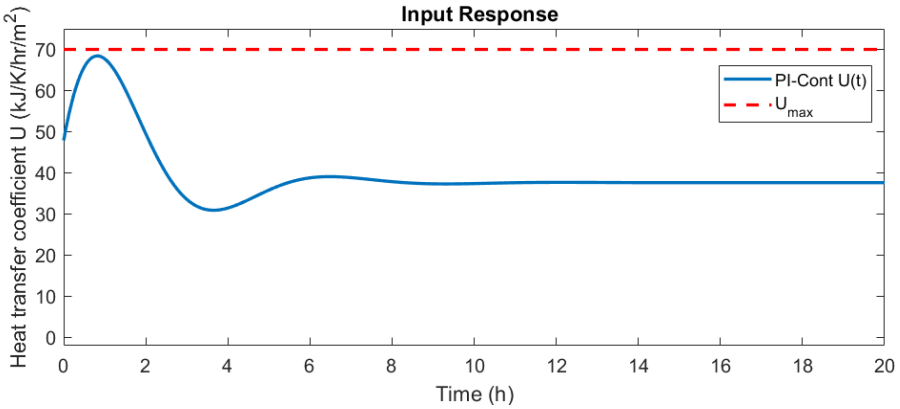


Figure 20: The DSM in units of reactor temperature (K) for U_{max} 70, with disturbance input included for P and PI Controllers with $[k_c]$={ -25, -55, -75} and $[\tau_i]$= {2, 0.75}

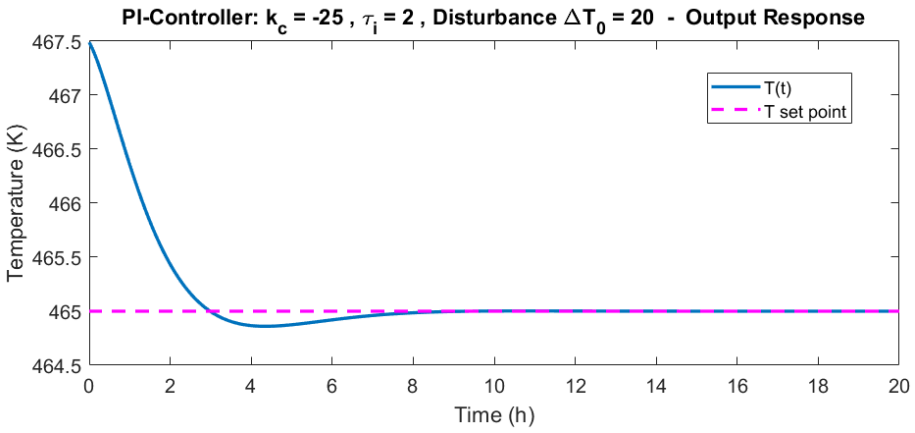


(i). Output response

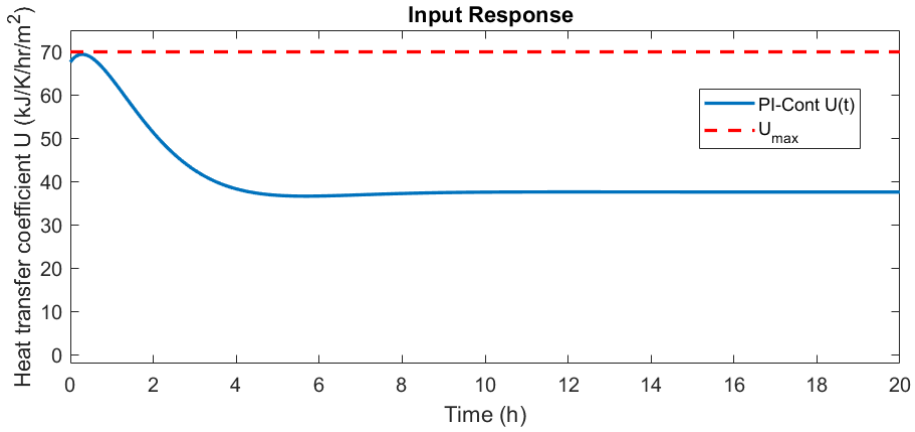


(ii). Input response

Figure 21: (i). Output response T(t) and (ii). Input response U(t) to a +20 K step disturbance in T_0 and initial impulsive disturbance that shifts T by 1.7 K. The PI-controller based closed-loop system with k_c of -25 and τ_i of 0.75 operating at 465 K.



(i). Output response



(ii). Input response

Figure 22: (i). Output response T(t) and (ii). Input response U(t) to a +20 K step disturbance in T_0 and 2.6 K initial impulsive disturbance in T. The PI-controller based closed-loop system with k_c of -25 and τ_i of 2 operating at 465 K.

The Table 2 below summarizes the results obtained for various U_{max}, k_c and τ_i for both P and PI control strategies. The results are shown for operating points 460 and 465 K operating points with disturbance input included. The DSM lies between 0 and 3.8 for the grid of design parameters investigated. As mentioned before, the margins of this range are low, but reasonable as it accounts for process dynamics under the possibility of sudden and adverse disturbances that were deliberately chosen as a representative of severe abnormal scenarios. In this paper, it is assumed that process should handle deviations in temperature up to +/- 2 K, that is, a minimum DSM of 2 K. As there are offsets present with P-only controllers, they will not be recommended for this process. Finally, under the assumption that U_{max} is too expensive of a choice for heat exchanger design, some design recommendations are highlighted in Table 2 that makes sense in the context of process safeness criterion.

Table 2: DSM in units of reactor temperature (K) for various design configurations

Type	k_c	τ_i	U_{max}	Steady state T: 465 K	Steady state T: 460 K
				DSM (K)	
P-Only	-25.00	∞	55	2.0	1.7
P-Only	-55.00	∞	55	0.9	0.8
P-Only	-75.00	∞	55	0.7	0.6
P-Only	-25.00	∞	70	2.6	2.3
P-Only	-55.00	∞	70	1.2	1.0
P-Only	-75.00	∞	70	0.9	0.8
P-Only	-25.00	∞	100	3.8	3.5
P-Only	-55.00	∞	100	1.7	1.6
P-Only	-75.00	∞	100	1.3	1.2
PI	-25.00	5	55	2.0	1.5
PI	-55.00	5	55	0.9	0.8
PI	-75.00	5	55	0.7	0.6
PI	-25.00	5	70	2.6	2.3
PI	-55.00	5	70	1.2	1.0
PI	-75.00	5	70	0.9	0.8
PI	-25.00	5	100	3.8	3.5
PI	-55.00	5	100	1.7	1.6
PI	-75.00	5	100	1.3	1.2
PI	-25.00	2	55	1.7	0.0
PI	-55.00	2	55	0.9	0.7
PI	-75.00	2	55	0.7	0.5
PI	-25.00	2	70	2.5	2.0
PI	-55.00	2	70	1.2	1.0
PI	-75.00	2	70	0.9	0.8
PI	-25.00	2	100	3.8	3.4
PI	-55.00	2	100	1.7	1.6
PI	-75.00	2	100	1.3	1.2
PI	-25.00	0.75	55	0.8	0.0
PI	-55.00	0.75	55	0.7	0.0
PI	-75.00	0.75	55	0.6	0.0
PI	-25.00	0.75	70	1.7	1.2
PI	-55.00	0.75	70	1.1	0.9
PI	-75.00	0.75	70	0.9	0.7
PI	-25.00	0.75	100	3.0	2.5
PI	-55.00	0.75	100	1.7	1.6
PI	-75.00	0.75	100	1.3	1.2

These recommendations require further refining and optimization before choosing the final design. There is a need for another yard stick to evaluate the other performance criterion. Prescreening of steady states done in the previous subsection, guarantees a minimum reactant conversion of 85%. Since the system is exothermic in nature, the reactant conversion percentage increases as the operating temperature increases. This will lead to choosing 465 K as the most favorable steady-state. The PI controller based designs ensures there are not any offsets. The simulations show that there are not any oscillations observed in time responses for the integral times of 5 and 2 unlike

for the integral value of 0.75. It is also assumed that the heat exchanger design with U_{max} of 100 kJ/K/hr/m^2 is too expensive of a choice. Based on the observations for the parameter grid analyzed, a final design that could be recommended for this case study is as follows:

Steady state temperature: 465 K
Heat exchanger design parameter (U_{max}): 70 kJ/K/hr/m^2
PI controller gain (k_c): -25
PI controller integral time (τ_i): 2

The above design parameters will be used in the next subsection for illustrating the reference governor concept.

5.2.3 Reference governor implementation using DSS for managing large set point changes during an upset scenario

The reference governor concept is implemented on this system to demonstrate its use in managing any sudden and large set point change that arise during abnormal events. It is illustrated for the system that is based on the final design recommended in the previous subsection. Figure 23 shows the DSS evaluated for the system operating at 465 K with a U_{max} of 70 kJ/K/hr/m^2 and a PI-Controller based closed-loop system with k_c of -25 and τ_i of 2. The 3 dimensional DSS shows the effect of the temperature set point on the DSS. From the figure, it can be inferred that the feasible and safe set points that can be handled by this system lie between 455 and 475 K.

During the event of a downstream upset scenario associated with a reactor effluent heat exchanger malfunction, it is required that the reactor operating temperature is decreased from 465 K to 457 K. In order to test the performance of the reference governor scheme in adverse conditions, the system is assumed to be under a persistent disturbance of 20 K in T_0, in addition to the downstream upset situation. The time responses of the output and input variables while using only a PI controller is shown in Figure 24. The time responses of the output, input and the reference governor parameter (K in eq. (28)) for the system with PI controller and the reference governor scheme is shown in Figure 25.

Figure 24 shows that the process runs with control input saturation for over 15 h before reaching the new steady-state. This is avoided in the case with the reference governor that eliminates the effect of disturbance while also taking the system to the new steady state in 10 h, without sustained input constraint violation. The control input responses from the two cases clearly demonstrate the benefits of using the reference governor to handle sudden and large set point changes.

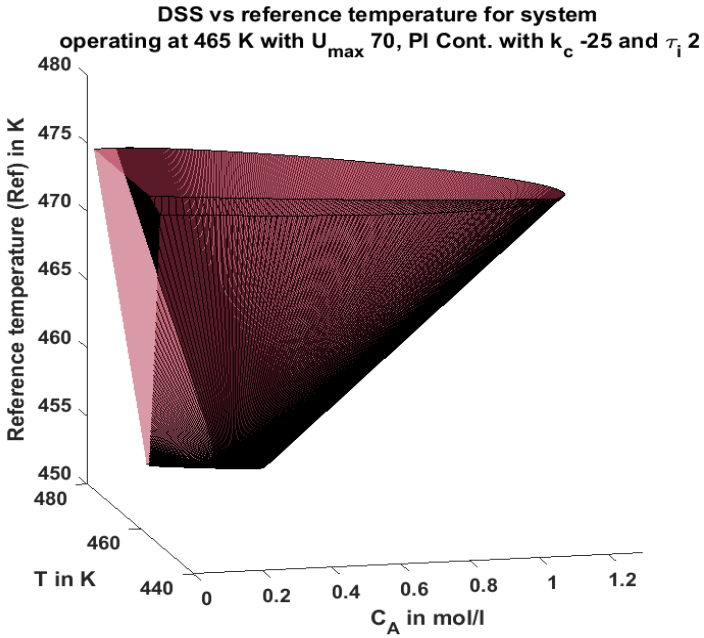
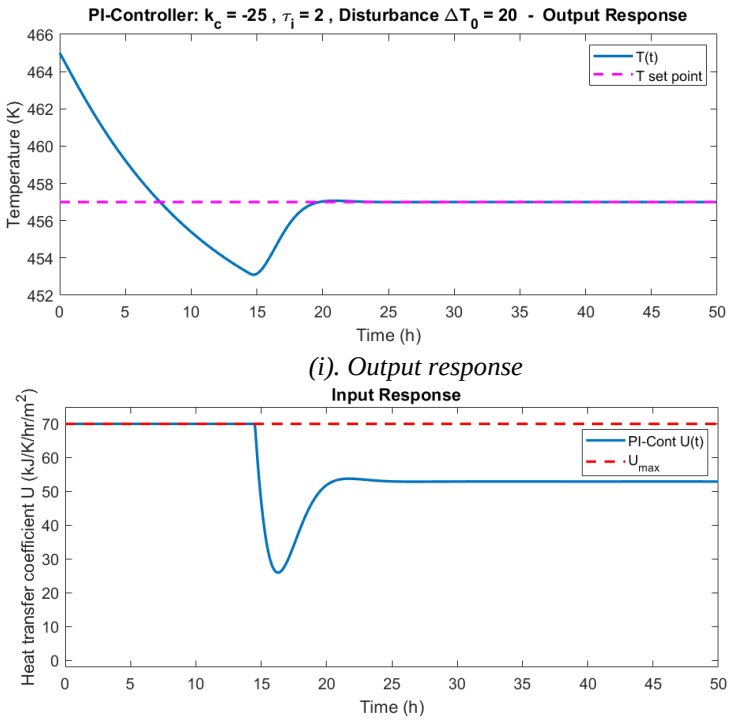


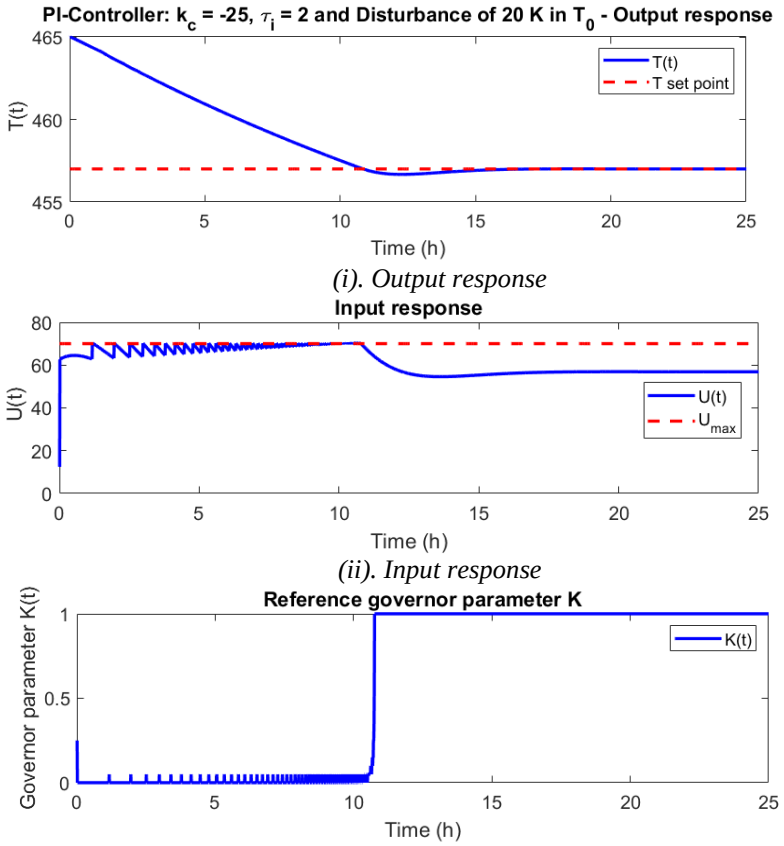
Figure 23: DSS for reference governor implementation. Process operating at steady state temperature of 460 K based on a PI controller with k_c -25, τ_i 2 and U_{max} 70.



(i). Output response

(ii). Input response

Figure 24: Set point change without reference governor. (i). Output response T(t) and (ii). Input response U(t) under a +20 K step disturbance in T_0 for the PI-controller based closed-loop system with k_c of -25 and τ_i of 2 operating at 465 K.



(i). Output response

(ii). Input response

(iii). Reference governor parameter K(t)

Figure 25: Set point change with reference governor. (i). Output response T(t), (ii). Input response U(t) and (iii). Governor parameter K(t) (in eq. (28)) under a +20 K step disturbance in T_0 for the PI-controller based closed-loop process with k_c of -25 and τ_i of 2 operating at 465 K.

6 Conclusions and future directions

An approach to design the process control system with safety as the primary target is proposed in this paper. The proposed approach explores an alternative perspective of safety-centered design as opposed safety as secondary considerations. The conceptualization of dynamic safe sets (DSS) and dynamic safety margins (DSM) and its application in control system are the key contributions of this paper.

The DSS is a collection of safe initial states that guarantee the satisfaction of safety constraints at present and future time instants, while also accounting for effects of unknown bounded disturbances. Existing theoretical concepts from systems literature were used to determine and evaluate the DSS that is an n-dimensional closed set. The DSM was conceptualized to quantify the size of the DSS that can be used to compare different designs. It is defined as the maximum radius of the n-dimensional ball centered at the steady state that completely lies within the DSS. The dynamic safety margin provides a measure of how resilient the closed-loop system is towards handling disturbances that are not accounted for, system faults and failures, measurement sensor noises and model uncertainties. An approach to design a maximally safe process control system based on the DSS and DSM concepts was proposed.

The proposed approach was tested on an exothermic CSTR as a representative example for systems with exothermic reactions with cooling system and control system. It was possible to select safe

set point that provided a relatively larger dynamic safety margin. The steady state reactor temperature of 465 K was identified as the favorable set point for this case study. The dynamic responses of the process under disturbances validated the concepts as they could safely eliminate effects of both initial impulsive disturbances in reactor state variables and persistent disturbances in feed temperature. The DSM evaluated for the normalized states, provided insights on the resilience of the process towards other disturbances and failures that were not accounted for in the DSS calculations. The control system design affected the DSM significantly. It was seen that for P controllers, larger absolute values of gains that provided smaller offsets but reduced the DSM significantly. In one case, using a gain of -75 for a P-controller provided a DSM of 0.5 K, that is even a 0.5 K initial perturbation in reactor temperature could push the process to unsafe operation zone. For PI controllers, the DSM decreased with increasing integral action as expected. The final design recommendations were made such that the DSM (2 K in units of temperature) was acceptable, a reasonable controller performance (no oscillatory behavior) was attained and cooling system U_{max} was realistic and affordable. The reference governor scheme also helped in enhancing process safety for dealing with abnormal situations that demand sudden large set point changes in the process. The time responses under downstream upset scenario showed superior performance when compared to the process without reference governor. The use of reference governor avoided sustained constraint violations and provided relatively quicker response.

In the future, DSS applications in other areas of plant design and operation will be explored. A potential application of the DSS envisioned is in process monitoring once the control system design and reference governor scheme have been implemented. The DSS can be integrated with the alarm system to alert the operator when the process lies outside of the safe set. This will allow for the operator to troubleshoot and take proactive measures to prevent the process from violating constraints. The system faults not accounted for while designing, such as sensor faults, actuator faults and equipment unavailability, can be included in the form of additional constraints. The dynamic safe sets evaluated for the different faulty scenarios can be coupled with a fault diagnosis system to automatically update the DSS.

The concept of safety margin is used in several engineering disciplines and sometimes mandated by law to adhere to safety margin standards. For example, a scale factor of 11 is used for elevators and a factor of safety of 2 is used for each structural member in building construction. It would be useful if there could be some design specifications on safety margins that is developed for chemical processes. The DSM is a quantitative and dynamic measure of characterizing safety performance that has the potential to be viewed as *the margin* for chemical processes. In future, the proposed approach will be applied to several chemical engineering systems that are safety critical to develop specific design specifications for DSM. Potential systems for investigations include, polymerization reactors and large-scale plants often used as test beds by the control academic community [26-28]. The results from these investigations will be used to develop fundamental engineering guidelines for safety-centered process and control system design.

7 References

1. Mannan, M.S., S. Sachdeva, H. Chen, O. Reyes-Valdes, Y. Liu, and D.M. Laboureur, *Trends and Challenges in Process Safety*. 2015. p. 3558-3569.
2. Willey, R.J., *Layer of Protection Analysis.* Procedia Engineering, 2014. **84**: p. 12-22.
3. Pasman, H.J., S. Jung, K. Prem, W.J. Rogers, and X. Yang, *Is risk analysis a useful tool for improving process safety?* Journal of Loss Prevention in the Process Industries, 2009. **22**(6): p. 769-777.

4. Mannan, S., *Lees' Process Safety Essentials : Hazard Identification, Assessment and Control*. 2013, Oxford, UNITED STATES: Elsevier Science & Technology.
5. Halim, S.Z., S. Janardanan, T. Flechas, and M.S. Mannan, *In search of causes behind offshore incidents: Fire in offshore oil and gas facilities.* Journal of Loss Prevention in the Process Industries, 2018. **54**: p. 254-265.
6. Saada, R., D. Patel, and B. Saha, *Causes and consequences of thermal runaway incidents—Will they ever be avoided?* Process Safety Environmental Protection, 2015. **97**: p. 109-115.
7. Leveson, N.G. and G. Stephanopoulos, *A system-theoretic, control-inspired view and approach to process safety.* AIChE Journal, 2014. **60**(1): p. 2-14.
8. Qin, S.J. and T.A. Badgwell, *A survey of industrial model predictive control technology.* Control Engineering Practice, 2003. **11**(7): p. 733-764.
9. Darby, M.L. and M. Nikolaou, *MPC: Current practice and challenges.* Control Engineering Practice, 2012. **20**(4): p. 328-342.
10. Morari, M. and J.H. Lee, *Model predictive control: past, present and future.* Computers & Chemical Engineering, 1999. **23**(4-5): p. 667-682.
11. Albalawi, F., A. Alanqar, H. Durand, and P.D. Christofides, *A feedback control framework for safe and economically-optimal operation of nonlinear processes.* AIChE Journal, 2016. **62**(7): p. 2391-2409.
12. Albalawi, F., H. Durand, and P.D. Christofides, *Process operational safety using model predictive control based on a process Safeness Index.* Computers & Chemical Engineering, 2017. **104**: p. 76-88.
13. Ahooyi, T.M., M. Soroush, J.E. Arbogast, W.D. Seider, and U.G. Oktem, *Model-predictive safety system for proactive detection of operation hazards.* AIChE Journal, 2016. **62**(6): p. 2024-2042.
14. Gilbert, E.G. and K.T. Tan, *Linear systems with state and control constraints: The theory and application of maximal output admissible sets.* IEEE Transactions on Automatic control, 1991. **36**(9): p. 1008-1020.
15. Kolmanovsky, I. and E.G. Gilbert. *Maximal output admissible sets for discrete-time systems with disturbance inputs*. in *Proceedings of 1995 American Control Conference-ACC'95*. 1995. IEEE.
16. Gilbert, E.G., I. Kolmanovsky, and K.T. Tan, *Discrete-time reference governors and the nonlinear control of systems with state and control constraints.* International Journal of robust nonlinear control, 1995. **5**(5): p. 487-504.
17. Gilbert, E.G., I. Kolmanovsky, and K.T. Tan. *Nonlinear control of discrete-time linear systems with state and control constraints: A reference governor with global convergence properties*. in *Proceedings of 1994 33rd IEEE Conference on Decision and Control*. 1994. IEEE.
18. Gilbert, E.G. and I. Kolmanovsky, *Fast reference governors for systems with state and control constraints and disturbance inputs.* International Journal of Robust Nonlinear Control: IFAC-Affiliated Journal, 1999. **9**(15): p. 1117-1141.
19. Gutman, P.-O. and M. Cwikel, *Admissible sets and feedback control for discrete-time linear dynamical systems with bounded controls and states.* IEEE transactions on Automatic Control, 1986. **31**(4): p. 373-376.
20. Kolmanovsky, I. and E.G. Gilbert, *Theory and computation of disturbance invariant sets for discrete-time linear systems.* Mathematical problems in engineering, 1998. **4**(4): p. 317-367.

21. Hirata, K. and Y. Ohta. *The maximal output admissible set for a class of uncertain systems*. in *2004 43rd IEEE Conference on Decision and Control (CDC)(IEEE Cat. No. 04CH37601)*. 2004. IEEE.
22. Lombardi, W., A. Luca, S. Olaru, and S.-I. Niculescu. *State admissible sets for discrete systems under delay constraints*. in *Proceedings of the 2010 American Control Conference*. 2010. IEEE.
23. Wang, C. and C.J. Ong, *Constraint-admissible sets for systems with soft constraints and their application in model predictive control.* International Journal of robust nonlinear control, 2012. **22**(11): p. 1229-1243.
24. Manthanwar, A., V. Sakizlis, V. Dua, and E. Pistikopoulos, *Robust model-based predictive controller for hybrid system via parametric programming*, in *Computer Aided Chemical Engineering*. 2005, Elsevier. p. 1249-1254.
25. Choi, J., H.S. Ko, and K.S. Lee, *Constrained H∞ optimal control of chemical processes.* IFAC Proceedings Volumes, 2001. **34**(25): p. 591-595.
26. Ricker, N.L., *Decentralized control of the Tennessee Eastman challenge process.* Journal of Process Control, 1996. **6**(4): p. 205-221.
27. Ricker, N., *Optimal steady-state operation of the Tennessee Eastman challenge process.* Computers & Chemical Engineering, 1995. **19**(9): p. 949-959.
28. Venkidasalapathy, J.A., M.S. Mannan, and C. Kravaris, *A quantitative approach for optimal alarm identification.* Journal of Loss Prevention in the Process Industries, 2018. **55**: p. 213-222.