Contents lists available at ScienceDirect

Journal of Process Control

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

Model-predictive fault-tolerant control of safety-critical processes based on dynamic safe set

Ritu Ranjan, Costas Kravaris *

Artie McFerrin Department of Chemical Engineering, Texas A&M University, College Station, TX, United States

ARTICLE INFO

Keywords:
Fault tolerant control
Model-based control
Process safety
Nonlinear process
Fault detection
Isolation and estimation
Dynamic safety margin
Process control

ABSTRACT

Industrial systems and chemical plants heavily rely on automation and control systems for seamless operations. However, the susceptibility of these systems to various faults poses threats to processes, leading to economic losses and safety risks. Here, a robust fault-tolerant control (FTC) strategy is developed that can take proactive measures during faults involving in-time activation of a backup controller, to ensure that the system remains within safe operational limits. It is based on the Dynamic Safe Set (DSS) which is the set of initial process states that meet safety constraints at all times, and the dynamic safety margin (DSM) which is the minimum distance from the DSS boundary. For just-in-time corrective action, a critical fault function is introduced, defined as the time required by the system to cross the DSS boundary under the nominal controller only. This critical fault function is calculated offline and is integrated with a real-time fault size estimation to formulate the controller reconfiguration logic to keep system within DSS. A linear functional observer is used to estimate fault size, combined with a predictive scheme, to enhance robustness during the transient period of fault estimation. This configuration avoids unnecessary control actions while ensuring timely intervention. The proposed FTC strategy is tested on an exothermic Continuous Stirred Tank Reactor (CSTR) case study. The results demonstrate the strategy's effectiveness in handling process faults, ensuring both stability and safety constraints are met. Thus, this paper contributes to the advancement of FTC ensuring the resilience of industrial systems in the face of unforeseen challenges.

1. Introduction

Modern-day industrial processes which are inherently nonlinear and multivariable interacting systems under closed-loop control are highly complex due to increased high performance demand and production efficiency requirements. The increasing complexity make systems more and more vulnerable to faults and malfunctions [1]. The consequences of such failures can be severe, leading to detrimental outcomes that can affect economic, safety, environment, and overall operational efficiency. Therefore, resilience to system malfunctioning to maintain safety is crucial requirement of today's industrial automation [2]. In order to make system gain such ability, a fault tolerant control design needs to be considered to ensure an efficient and timely response to mitigate safety risks [3]. More precisely, a closed-loop control system that can accommodate component (actuators, sensors, process and controller) failure automatically while maintaining desirable performance and system overall stability is known as fault tolerant control systems (FTCS) [4,5]. The survey papers in [6–8] have reviewed the development and advancement of active and passive FTCS and investigated the challenges and advantages of them.

The active FTCS consists of the following subsystems: Fault detection and isolation (FDI) module, a reconfiguration mechanism and a reconfigurable controller. It reacts in real-time by immediately reconfiguring the controller based on the information provided by FDI module. On the other hand, in a passive FTCS design, potential failure modes are assumed first, and the controller is synthesized to deal with these failure modes together with the normal operating conditions [6]. It refers to a control system that is inherently robust to certain predefined faults or disturbances without the need for dynamic fault compensation. Thus, the "passive" in passive FTCS refers to a control strategy that does not actively reconfigure or adjust itself in response to detected faults. The adaptive nature of active FTCS equip it with a greater capability to handle different types of faults, making it more applicable and flexible as compared to the passive approach which can handle only predefined fault sets used in its design stage. Thus, passive FTCS becomes less effective and suffers from conservative performance as the number of

* Corresponding author.
E-mail address: kravaris@tamu.edu (C. Kravaris).

https://doi.org/10.1016/j.jprocont.2024.103329
Received 11 August 2024; Received in revised form 30 September 2024; Accepted 21 October 2024
Available online 7 November 2024

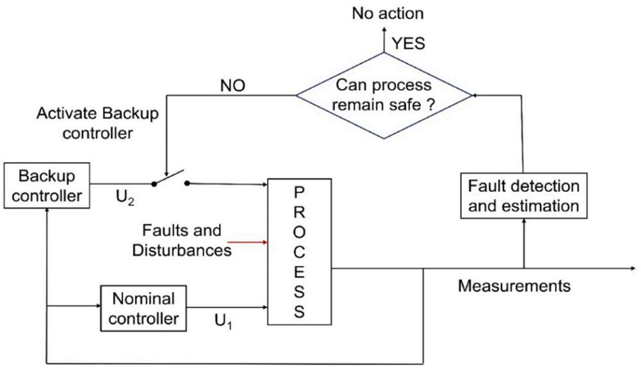

Fig. 1. The FTC structure.

potential fault cases increases. The robust control methods such as quantitative feedback theory, H_∞ norm optimization method, μ synthesis, Linear-Quadratic control, variable structure control are used for passive FTCS whereas strategies of active FTCS are based on switching and tuning, control law rescheduling, adaptive control, parameter space approach, eigen structure assignment [9].

The success of the active FTC mainly depends on the accuracy of the FDI unit in the design structure. Over the last three decades, extensive research has been devoted in developing FDI methods to integrate with FTCS. There are several techniques including model based (Kalman filter, Unknown input observer) and knowledge based (statistical and non-statistical analysis) for FDI [10,11]. The authors of these works have mentioned advantages and disadvantages of individual FDI methods. The observer-based fault diagnosis for designing residual generation and residual evaluation is the most common technique where the process model is incorporated in an observer to deliver an estimate by comparison of output with measurements [12]. The survey papers [13,14] briefly outline the theoretical framework mostly based on Luenberger observer for fault diagnosis. The existence conditions of functional observer for linear systems are derived in [15]. Also, the concept and design of functional observers for fault detection which has the advantage over full-state observers is provided in [16]. As most of the industrial process are nonlinear, focus to design nonlinear observer for FDI is considered in [17,18]. The exact observer error linearization is the powerful method for designing nonlinear observer [17,18]. Recently, there have been efforts to develop data-driven FDI approaches whenever raw historical data are available from the distributed control system. The various data-driven approach including Bayesian network, random forest, neural network and their challenges and opportunities for smart fault diagnosis are discussed in [19,20].

Once the fault information is available from FDI, online controller parameter adaptation and switching to alternative controllers to accommodate faults is common in active FTCS. Since PID controllers dominate industry for half a century, several auto-tuning methods based on minimum variance, pole placement or linear quadratic gaussian design methods and adaptive parameter estimation is proposed. The auto-tuning algorithm is combined with adaptive neural network (NN) model to learn the post-faults dynamics to tune PID parameters online [21]. However, due to the limitations of PID under multivariable interaction, most of the works focused on integrating advanced controllers like model predictive control (MPC) with FTC scheme [22–24]. The authors of these works employ Lyapunov based techniques to handle uncertainty, constraints and explicitly characterize the stability region from level sets associated with each fallback control configuration for switching policy during faults. Recently, more studies are focused on the application of FTC for nonlinear system integrating with FDI [25–30]. The assumption of these methods is that the states need to be in stability region of any backup controller at the time of fault. To solve the problem of non-existence of stability region for any backup controller during fault, a safe parking method is proposed in [31–34] where the system is maintained at temporary equilibrium point until fault rectifies. Despite these advancements, the industrial application of these methods is challenged by the complexity of integrating MPC, whose interpretability and trust is questioned by industry [35] and the conservative estimate of Lyapunov stability region for each controller that can restrict the flexibility and responsiveness of the control system.

More recently, a simple concept dynamic safety margin (DSM) defined as minimum distance of current states from safety boundaries is used in designing the control strategy including MPC to achieve FTCS [36–40]. Also, dynamic safe set (DSS) defined as maximal output admissible set is considered for designing control schemes capable of handling disturbances in safety-critical processes [41]. The DSS is leveraged for developing FTC strategy used as overall safety region for the overall process satisfying safety constraints where the goal of the control configuration is to keep the system within that region all the time, even in the presence of faults based on DSM [42].

The conclusion from reviewing available literature is that it is still an open question how to build a general and practical FTCS design method providing controller reconfiguration just in time, which is crucial for safety-critical processes. The just-in-time controller reconfiguration happens precisely at the time it is needed, ensuring safe operation, while avoiding unnecessary actions that could impact performance. It does not proactively reconfigure the controller unless necessary. This study focuses on overcoming the limitations of existing Fault-Tolerant Control Systems (FTCS) methods, where only FDI is integrated with controller reconfiguration techniques, mostly based on Lyapunov functions, to maintain stability. In the presence of nonlinear dynamics and multiple interacting variables, constructing the Lyapunov stability region, often conservative for each controller, is challenging. Also, without estimating fault size, the control system could overreact, potentially leading to unnecessary corrective actions or premature trips that result in economic losses (see [43] for an analysis of the economic operability of a processing plant in the presence of faults is essential when considering the balance between safety and productivity). The solution proposed in this paper involves the integration of a single DSS and a fault identification module in transient phase. Keeping the system within DSSs guarantees satisfaction of all safety constraints, considering the capabilities of both nominal and backup controllers. As DSS keeps the system close to its operating parameters, it prevents the process from reaching alarm states that would otherwise trigger the emergency shutdown system (ESD). By avoiding trips that result in costly downtimes, the DSS helps maintain economic efficiency while ensuring that safety-critical thresholds are not breached. The proposed approach simplifies the FTC control strategy and improves its adaptability to various fault scenarios. The switching criteria for controller reconfiguration are based on fault size estimated from a linear functional fault estimator. Using fault estimator in transient stage helps in taking corrective action before system crosses the DSS boundary and avoids any unnecessary control action in presence of faults. Thus, the main contribution of this paper is an active FTC scheme which is more robust and flexible, facilitating the applicability in real-world industrial settings as compared to existing FTC schemes mentioned in the literature. It provides just-in-time controller reconfiguration on the basis of fault size, keeping the system within DSS. The FTC strategy aims to maximize safety and performance while minimizing unnecessary control actions. Specifically, this work implements the proposed active FTC scheme for an exothermic CSTR focusing on faults such as feed overheating, which pose significant safety risks.

This paper is organized as follows: Section 2 presents the problem formulation to develop FTC strategy of a nonlinear process system in presence of faults. Section 3 reviews necessary background on functional observers for fault estimation as well as DSS and DSM concepts to calculate safe operating set and a safety index. Section 4 outlines the necessary offline information that will be used by the proposed FTC system. Section 5 details the proposed FTC strategy, including the real-time predictive feature and decision logic. Section 6 implements the

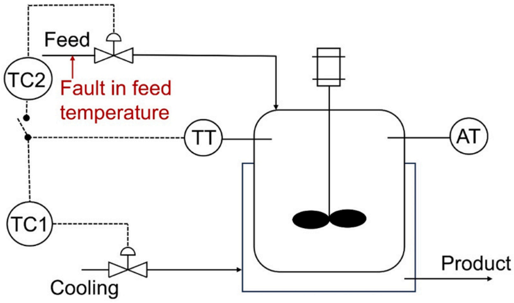

Fig. 2. Schematic of CSTR process.

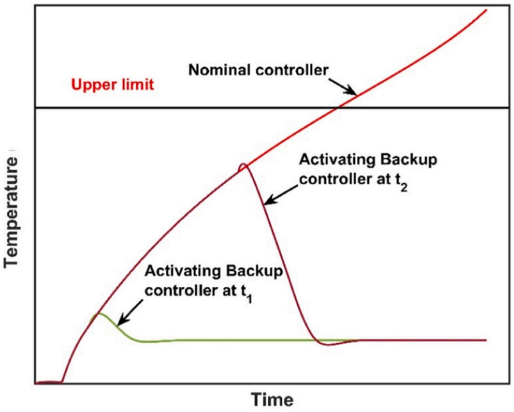

Fig. 3. Trajectory when BC is activated at different time when fault occurs.

proposed FTC approach on a safety-critical process involving an exothermic reaction handled in a continuous stirred tank reactor (CSTR). Section 7 discusses the simulation results for different fault types and sizes. Section 8 outlines conclusions and future directions.

2. Problem statement

In safety-critical processes, maintaining system stability and predefined constraints in the presence of faults and disturbances is paramount. An active FTC structure as shown in Fig. 1 ensures an efficient and timely response to faults in order to keep the system within safety limits. The components of an active FTC structure include fault detection and estimation (FDE) module, nominal and backup controller, and a controller accommodation law (decision logic). The process has nominal controller with manipulating input U_1, operating alone under fault-free conditions, and a backup controller with manipulating input U_2 that only gets activated in response to faults. When a fault occurs, the FDE module detects, isolates, and estimates the size of fault. Based on the fault size, the decision logic, in general, determines whether the system can remain safe at all future times. If not, the nominal controller is accommodated with activation of backup controller to keep system within safe operating region.

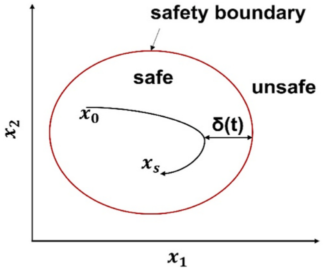

Fig. 4. Safe operating region.

To help define the problem of designing a FTC system, a motivating example of a chemical reactor where fault in feed temperature happens as shown in Fig. 2 is briefly discussed here. A well-mixed, non-isothermal CSTR where an exothermic reaction takes place is considered. For exothermic reactions which release heat, the temperature must be precisely controlled to prevent runaway reaction that has the potential to cause explosive accidents. Faults such as cooling system failures or unexpected feed temperature increase can cause the reactor temperature to rise uncontrollably, posing severe safety risks. An active FTC strategy is essential to maintain temperature within safe operating limits even in the presence of faults. The control strategy would involve the use of a nominal controller (NC) manipulating cooling, designed for normal operating conditions to handle small faults and disturbances. On the other hand, the backup controller (BC) manipulating feed flowrate is to be designed to handle large-size faults size and to be only activated in response to faults, operating together with NC. The BC should be more aggressive, aiming to maintain the system within a safe operating region, but should not be activated unnecessarily, as changes in the feed flow rate might drive the reactor away from proper design conditions. As shown in Fig. 3, in the presence of a fault, the temperature starts increasing and crosses the safety upper limit when NC alone is active. Therefore, BC is needed to provide additional control action to counteract the fault and keep system below the upper limit. This combined controller action approach helps to maintain safety constraints in presence of both small and large faults. Activating the backup controller at time t_2 which is later than t_1, increases the potential of the system trajectory crossing the upper limit. It highlights the importance of the activating the BC in a timely manner. Delays in activation can result in the system crossing safety boundaries, and this indicates the need for timely intervention via the BC to ensure the system remains within the safe operating region.

Another important factor is fault size, since it determines the speed by which the system might cross the upper limit; larger faults drive the system more quickly out of the safe operating region. For smaller fault size, it is not needed to activate BC as it can be handled by NC. So, it is important to estimate the fault size for determining proper activation time for the BC to avoid any unnecessary actions. In practice, the fault estimator takes time to converge, and waiting until it converges, might be too late. Therefore, the fault estimate must be utilized in transient, even though it might be underestimating the fault size. This difficulty motivates to use an extra online indicator to provide a quantitative measure of safeness, aiding in the timely activation of BC. A potential indicator, which will be discussed in Section 3.2, is the dynamic safety margin (DSM) that measures how far the system state is from a specified safety boundary. In our approach, the safe operating region will be the Safe Operating Set (SOS) defined in Section 4.1, which is a positively invariant set and stable in the sense of Lyapunov stability. The meaning of the safe operating region is that as long as the system operates within this region, all the safety constraints are satisfied. In Fig. 4, the system trajectory starting from the initial condition x_0 ends at the steady state x_s, traversing the state space with varying distance $\delta(t)$ from the safety boundary. As long as the trajectory remains within the set, the system is safe, but if it crosses the safety boundary, it enters an unsafe territory. The DSM is the distance of the current state of system from the safety boundary i.e. $\delta(t)$ shown in the Figure in this case.

The size of the safe region shown in Fig. 4 is expected to decrease as fault size increases, and may even become an empty set under the nominal controller alone, when the fault is too large. However, including the backup controller, could result in a reasonably-sized safety region even for large faults. As long as the fault size can be estimated, a decision can be made whether and when the backup controller should be activated: not unnecessarily and not too late. The switching must happen before the system is ready to cross the safety boundary, so that the combined action of nominal and backup controllers can keep it safe at all times. The goal of the proposed FTC strategy is to keep system safe in the presence of faults and disturbances by activating the backup controller in optimum only when necessary and just-in-time.

3. Background

In this section, a brief necessary review of two key tools is provided that are critical to the proposed fault-tolerant control (FTC) strategy. These are: (a) functional observers for detection, isolation, and estimation of the fault, to assess its potential impact on system performance and (b) the dynamic safe set (DSS) and dynamic safety margin (DSM) to ensure that the system's trajectory remains within specified input and output constraints, even in the presence of faults or disturbances, and this will enable defining the Safe Operating Set (SOS) in the next section.

3.1. Functional observer for fault estimation

Consider a nonlinear process that could be subject to faults and disturbances, of the form:

$$\frac{dx}{dt} = F(x) + G(x)f + E(x)W \tag{1}$$

$$y = H(x) + J(x)f + K(x)W \tag{2}$$

where $F(x), G(x), E(x), H(x), J(x), K(x)$ are smooth nonlinear functions, $x \in \mathbb{R}^n$ stands for stands for the state vector, $y \in \mathbb{R}^p$ are the output measurements, $W \in \mathbb{R}^m$ is a disturbance, $f \in \mathbb{R}$ is a potential fault acing on the system. Without loss of generality, f is understood to be nonnegative, with $f = 0$ indicating no fault and $f = f_{\max}$ indicating complete failure. The dynamics of the fault can be assumed to originates from a linear exo-system of the form:

$$\frac{dx_o}{dt} = Rx_o \tag{3}$$

$$f = Mx_o \tag{4}$$

where $x_o \in \mathbb{R}^{n_o}$ and R, M are constant matrices. Examples of such faults are ramp ($R = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, M = [1\ 0]$) and step ($R = 0, M = 1$) which will be considered in our case study. The linear functional observer is built for estimating fault f is [44]:

$$\frac{d\hat{\xi}}{dt} = A\hat{\xi} + By \tag{5}$$

$$\hat{f} = C\hat{\xi} + Dy \tag{6}$$

The observer has the following properties:

- $\hat{f} - f$ asymptotically approaches zero, under any initial conditions
- $\hat{f}$ is disturbance-decoupled, i.e. unaffected by W

Such observer can be designed if and only if there exist constant row vectors called parity vectors $\beta_o,\ \beta_1, \ldots \beta_\nu\ \in \mathbb{R}^p$ satisfying:

$$\begin{aligned} &L_{Fe}^{\nu}(\beta_o(H(x) + J(x)Mx_o\,)\,) + \quad L_{Fe}^{\nu-1}(\beta_1(H(x) + J(x)Mx_o\,)\,) + \ldots \\ &\quad + L_{Fe}(\beta_{\nu-1}(H(x) + J(x)Mx_o\,)\,) + (\beta_\nu(H(x) + J(x)Mx_o\,)\,) \\ &\quad = M(R^\nu + \alpha_1 R^{\nu-1} + \ldots + \alpha_{\nu-1}R + \alpha_\nu I)x_o \end{aligned} \tag{7}$$

$$where L_{Fe} = \quad \sum_{i=1}^{n} F_k(x)\frac{\partial}{\partial x_k} + Mx_o\sum_{i=1}^{n} G_k(x)\frac{\partial}{\partial x_k} + \sum_{i=1}^{n_o} R_k x_o \frac{\partial}{\partial x_{ok}}$$

and $\lambda^\nu + \alpha_1\lambda^{\nu-1} + \ldots + \alpha_{\nu-1}\lambda + \alpha_\nu$ is the characteristic polynomial of the linear error dynamics and disturbance decoupling conditions:

$$\sum_{l=0}^{\nu-k} L_E L_{Fe}^{\nu-k-l}(\beta_1(H(x) + J(x)Mx_o)) + \beta_{\nu-k+1}(K(x)) = 0 \tag{8}$$

$$k = 1, \ldots \nu$$

$$\beta_o(K(x)\,) = 0 \tag{9}$$

When the above conditions are satisfied, the linear functional observer of the form (5–6) with A, B, C, D matrices given by:

$$A = \begin{bmatrix} 0 & 0 & \cdots & 0 & -\alpha_\nu \\ 1 & 0 & \ldots & 0 & -\alpha_{\nu-1} \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \ldots & 1 & 0 & -\alpha_2 \\ 0 & \ldots & 0 & 1 & -\alpha_1 \end{bmatrix}, \quad B = \begin{bmatrix} \beta_\nu - & \alpha_\nu\beta_0 \\ \beta_{\nu-1} - & \alpha_{\nu-1}\beta_0 \\ \beta_{\nu-2} - & \alpha_{\nu-2} - \beta_0 \\ & \vdots \\ \beta_1 - & \alpha_1\beta_0 \end{bmatrix} \tag{10}$$

$$C = \quad [0 \quad 0 \quad \cdots \quad 0 \quad 1], \quad D = \quad \beta_0 \tag{11}$$

has all the required properties and the eigenvalues of A are the roots of the $\lambda^\nu + \alpha_1\lambda^{\nu-1} + \ldots + \alpha_{\nu-1}\lambda + \ \alpha_\nu$[44].

Under full state measurements, without sensor faults or disturbances ($y = x$), it is often possible to design a first-order ($\nu = 1$) functional observer. The design conditions are:

$$\beta_o(F(x) + G(x)Mx_o\,) + \beta_1 x = M(R + \alpha_1 I)x_o \tag{12}$$

$$\beta_1 E(x) = 0$$

and, if they are satisfied for some constant row vectors $\beta_o,\ \beta_1\ \in \mathbb{R}^n$, the dynamic system:

$$\frac{d\hat{\xi}}{dt} = -\alpha_1\hat{\xi} + (\beta_1 - \alpha_1\beta_0)x \tag{13}$$

$$\hat{f} = \hat{\xi} + \beta_0 x$$

is a functional observer.

The functional observer method presented here will form the basis of the fault estimation component of our proposed FTC algorithm. Note that the functional observer will have dynamics, and there will be a transient period until the fault estimate converges. The lag in fault estimation will be an issue to be addressed in the development of our FTC algorithm.

3.2. Quantification of dynamic safety: dynamic safe set (DSS) and dynamic safety margin (DSM)

The DSS is defined as a set of initial states that guarantee the satisfaction of all input/output safety constraints at any time in the future, even in the presence of unknown disturbances. It is a closed, positively invariant set calculated around a steady-state operating condition. To evaluate the DSS, the established theory of maximal output admissible sets is leveraged. The system dynamics of controlled nonlinear system are:

$$\dot{x} = F(x) + E(x)w \tag{14}$$

$$z_0 = \mathrm{h(x)}$$

where, $F(x), E(x), h(x)$ are smooth nonlinear functions, $x \in \mathbb{R}^n$ denotes the state, $z_0 \in \mathbb{R}^p$ denotes constrained output which is subject to bounded specified constraints $z_0(t) \in Z \subset \mathbb{R}^p$ and bounded disturbance inputs $w(t) \in W$ for all t. The maximal output admissible set (O_∞) can be defined in analogy to discrete nonlinear system[45]:

$$O_\infty = \{x(0) \in \mathbb{R}^n : z_0(t; x(0), w\,) \in Z, \forall \quad w(t) \in W, \forall \quad t > 0\,\} \tag{15}$$

The, finite characterisation of O_∞ has the property of Lyapunov stability(see proof in [46]). Although the criteria for finite

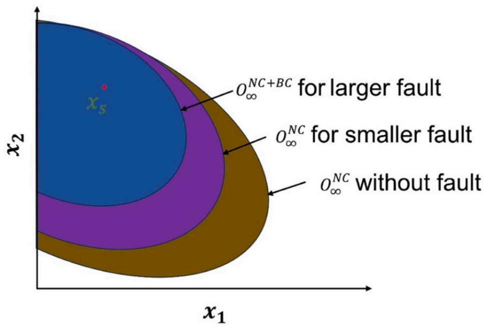
O_∞^{NC+BC} for larger fault
O_∞^{NC} for smaller fault
O_∞^{NC} without fault
x_s
x_2
x_1

Fig. 5. The effect of fault size on DSS.

characterisation of O_∞ are well established for discrete linear and nonlinear systems, there are no results available for continuous nonlinear systems [46]. In what follows, available results are reviewed for linear discrete-time systems, where specific ready-to-use computational algorithms are available for computing the O_∞. After linearization and discretization of our nonlinear system, these algorithms can provide a useful approximation of the O_∞.

Consider a linear, time-invariant, discrete system of the form (16), (17) which represents the closed loop system under a feedback controller, and is subject to bounded disturbance inputs $w(t) \in W$ and the output y must lie in a set Y in order to satisfy safety constraints.

$$x(t+1) = Ax(t) + Bw(t) \tag{16}$$

$$y(t) = Cx(t) + Dw(t) \tag{17}$$

$$y(t) = Cx(0) + Dw(0), \quad t = 0$$

$$y(t) = CA^t x(0) + \sum_{k=0}^{t-1} CA^{(t-k-1)} Bw(t) + Dw(t), \quad t \geq 1 \tag{18}$$

Then the maximal output admissible set [47,48]:

$$O_\infty = \{x(0) \in \mathbb{R}^n : y(t) \in Y, \forall \quad w(t) \in W, \forall \quad t \in \quad N^+\} \tag{19}$$

is the set of all initial conditions such that the output $y(t)$ lies within Y at all times, for all disturbance inputs $w(t)$ in W. In general Y is represented by inequalities:

$$Y = \{y \in \mathbb{R}^p : f_i(CA^t \mathrm{x}) \leq 0, \quad i = 1, \ldots, s\} \tag{20}$$

$$O_\infty = \{x \in \mathbb{R}^n : f_i(CA^t x) \leq 0, i \in \{1, \ldots, s\}, \quad t \in \{0, \ldots, t^*\} \quad \} \tag{21}$$

For O_∞ represented by (21) there exists a nonempty set of integers S*⊂ {1, …, s} and indexes ti*, i ∈ S*, such that t* = max {ti*, i ∈ S*}. The conditions necessary for finite determination and the recursive optimization algorithm for calculating O_∞.

$$O_{t+1} = O_t \cap \{x \in \mathbb{R}^n : (CA^t x) \in \mathrm{Y}\}, \quad O_0 = \{x \in \mathbb{R}^n : (Cx) \in \mathrm{Y}\} \tag{22}$$

The assumptions for finite determination of O_∞ for linear discrete system are: i) A is asymptotically stable ii) the pair C, A is observable iii) Y is bounded iv) $0 \in$ int Y[48]. Thus, finite characterisation of O_∞ includes Lyapunov stability property for both linear and nonlinear discrete systems [47–49]. The computational algorithm for set O_∞ provides safety boundaries for DSS, based on system dynamics, control strategies, and safety requirements. Typically, the safety critical constraints include bounds on output variables like the onset temperature of a runaway reaction, the level of liquid in vessel and the limits on controller actuator.

The safety boundary, DSS calculated around steady state is the set of linear inequalities given by[41]:

$$\mathrm{DSS} = \quad \{\phi_i(x) = a_i x - c_i \leq 0 | i = 1, \ldots, q\} \tag{23}$$

where q is the number of boundaries constraint. By providing a quantitative measure of how close a system is to violating safety constraints, the DSM helps in making timely decisions to maintain safe operations. It can be calculated as:

$$\mathrm{DSM}(\delta(t)) = \min \frac{c_{i-} a_i x}{||a_i||_2} \{> 0 \quad \textit{iff} \quad \phi_\mathrm{i}(\mathrm{x}) \quad \leq 0 \ \textit{and} < 0 \ \textit{iff} \ \phi_\mathrm{i}(\mathrm{x}) \geq 0\} \tag{24}$$

In the presence of different units of the state variables, appropriate normalisation is necessary to define a norm to calculate DSM [41]. The DSM is positive when system remains inside DSS whereas it becomes negative when trajectory crosses the DSS. At steady state DSM attains a constant value, and the rate of change of DSM becomes zero. Furthermore, when the system is approaching unsafe region, the rate of change of DSM becomes negative. Consequently, the sign of DSM or the rate of change of DSM exhibits sensitivity to the occurrence of faults. This sensitivity makes these parameters suitable for the development of switching rules for controller based on them. They serve as reliable indicators for identifying and responding to faults as the system operates.

The concept of DSS will enable defining the safe operating set in the next section, which will be a key element of our FTC algorithm, which will also involve DSM monitoring, once a large-size fault is detected.

4. Key offline information incorporated in the FTC algorithm

The objective of the proposed FTC algorithm will be to keep the system within an appropriately defined DSS, after the fault happens. This will be called the Safe Operating Set (SOS) and it will be a DSS for the combined NC + BC system in the presence of fault. The decision logic of the FTC algorithm will determine whether and when BC will be activated, given the transient fault size estimate from the functional observer, so that the system does not go outside the SOS. In particular, activation of BC will have to happen if and when the Dynamic Safety Margin (DSM), which is the distance from the boundary of SOS gets too small. Monitoring of the DSM will be initiated when the fault size estimate grows too fast as a function of time, and exceeds a certain threshold level. This threshold will be called Critical Fault Function (CFF) and it will be a function of the time elapsed after the fault occurrence.

Both the SOS and the CFF will have to be calculated offline and will be like design parameters of the proposed FTC algorithm. They will be defined and discussed in the present section.

4.1. The Safe Operating Set (SOS)

Every control system has its own DSS, which depends on the absence or presence of a fault, and in particular on the fault size. As the fault size increases, the size of the DSS typically decreases. This is because larger faults require more aggressive corrective actions to maintain system stability and safety, thereby reducing the range of initial states that can be safely controlled. Under only the nominal controller, as the fault size increases, the DSS shrinks and may become empty when the fault is large enough. This is when the backup controller can make a difference: operating together with the nominal controller, it can provide a decent-size DSS, enabling the safe operation of the process despite the presence of a large fault. The situation is illustrated in Fig. 5. In the absence of fault, the nominal controller is designed with a comfortably large O_∞^{NC}, when there is a small fault O_∞^{NC} shrinks but might still be adequate, in the presence of a large fault O_∞^{NC} might be void, but the combined nominal plus backup controller actions can give a decent-size DSS, O_∞^{NC+BC}. Note that O_∞^{NC+BC}might be smaller than O_∞^{NC} under zero fault, but this not a problem as long as it gives enough “room” for the process to operate safely. The important aspect is that O_∞^{NC+BC} is strongly dependent upon the fault size, and it should be reasonably large irrespective of the fault

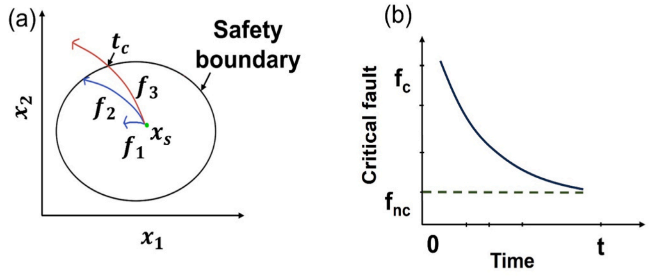

Fig. 6. Critical time-Critical fault definition.

size.

In practice, faults are bounded, $0 \leq f \leq f_{\max}$, where $f_{\max}$ represents the worst-case scenario of fault size (corresponding to 100 % failure a piece of equipment), and the combination NC+BC must be capable of protecting the system over the entire range of faults. For this reason, is defined the Safe Operating Set (SOS) as the set Φ which is the intersection of all DSS's over the entire fault range:

$$\Phi = \cap_{0 \leq f \leq f_{\max}} O_{\infty}^{NC+BC}(f) \tag{25}$$

where $O_{\infty}^{NC+BC}(f)$ denotes the DSS under a constant fault f when both NC and BC are active. Thus, the SOS reflects the capability of combined control effort of NC+BC to keep all constraints satisfied for any fault size within the fault range, and the NC and BC controllers should be designed so that Φ is large enough. The SOS will play a critical role on the proposed FTC algorithm: activation of the backup controller will happen while the system is still in SOS, so that it can remain in SOS in subsequent times.

It should be noted here that typically $O_{\infty}^{NC+BC}(f_1) \supset O_{\infty}^{NC+BC}(f_2)$ when $f_1 < f_2$, in which case $\Phi = O_{\infty}^{NC+BC}(f_{\max})$, and this facilitates the computation of Φ.

Note however that, as pointed out in Section 3.2, the computation of O_{∞} for general nonlinear systems is very challenging, and off-the-shelf computational algorithms are for discrete-time linear systems. This means that in practice, only an approximate O_{∞} can be obtained based upon the linearized and discretized system, which might represent an underestimation of the actual DSS [47]. Therefore, some fine-tuning of $f_{\max}$ will be needed through simulation, in order to improve the accuracy of the approximation of Φ. In reality, the system can tolerate faults that exceed $f_{\max}$ by a small degree due to the inherent conservatism in the DSS.

4.2. Critical fault function

It is necessary to develop a method to extract physically meaningful information from determined SOS that is relevant to find optimum time to activate BC. For this purpose, a concept of critical time (t_c) and critical fault (f_c) is proposed. Suppose a SOS is defined and only the nominal controller is active. When the system is initially at the design steady state (x_s) with no fault ($f = 0$), but suddenly there is a step fault of size f, the system will react to it and the system trajectory might cross the boundary of SOS. For small fault size it might not cross, but as the fault gets larger, it will cross at smaller and smaller times. As shown in Fig. 6 (a), the trajectory does not cross the SOS for smaller fault f_1 whereas increasing fault size lead to touch the boundary and further trajectory crosses the boundary for fault f_3. The time at which the system trajectory crosses the SOS when only nominal controller is operating during step fault is defined as critical time corresponding to that step fault, known as critical fault. Thus, for different critical fault size, there is a corresponding t_c which decreases as the step fault size increase.

Consider the closed loop system under the nominal controller only and suppose it is described by a state space model of the form:

$$\dot{x} = F(x) + G(x)f + E(x)W \tag{26}$$

Also, suppose that the system is initially ($t = 0$) at the design steady state, operating in the absence of fault or disturbances. Suddenly, a step fault happens, assuming a constant value of $f > 0$, for $t > 0$. Denote by $x(t;f)$ the solution of (26) and Φ the Safe Operating Set (SOS) defined in the previous subsection, and assume that Φ includes the design steady state. The time to cross the SOS boundary is defined as:

$$t_c = \sup\{\tau \in \mathbb{R}^+ | x(t;f) \in \Phi \forall \quad t \in [0, \tau]\} \tag{27}$$

In other words, the time to cross t_c is the largest time for which $x(t;f) \in \Phi \forall t < t_c$, with the understanding that if the entire state trajectory lies inside $\Phi \, \forall t > 0$, then $t_c = +\infty$.

The above defines a mapping between fault size and time to cross: $f \rightarrow t_c(f)$. Alternatively, one could define the inverse mapping $t \rightarrow f_c(t)$, where f_c is the fault size for which the time to cross is equal to t. f_c will be called critical fault size and $f_c(t)$ critical fault function.

Intuitively, it is expected that $t_c(f)$ is a monotonically decreasing function of f or equivalently that $f_c(t)$ is a monotonically decreasing function of t; this will be a standing assumption throughout this paper. Fig. 6(b) depicts the qualitative shape of the critical fault function.

The critical fault function $f_c(t)$ will be a critical ingredient of the proposed FTC algorithm, and it will have to be calculated offline. An analytical calculation will not be feasible in general; however, one can numerically calculate pairs (t_c, f_c), and thus generate a piecewise approximation of the function that will be used in the algorithm.

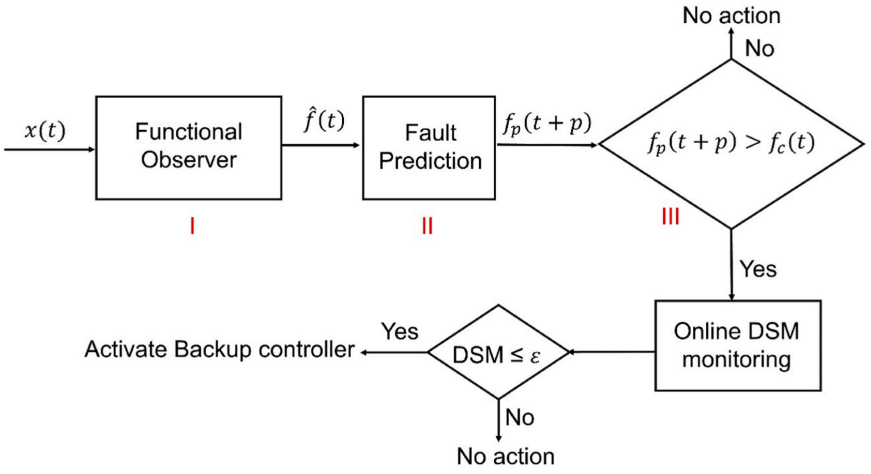

Fig. 7. The FTC algorithm.

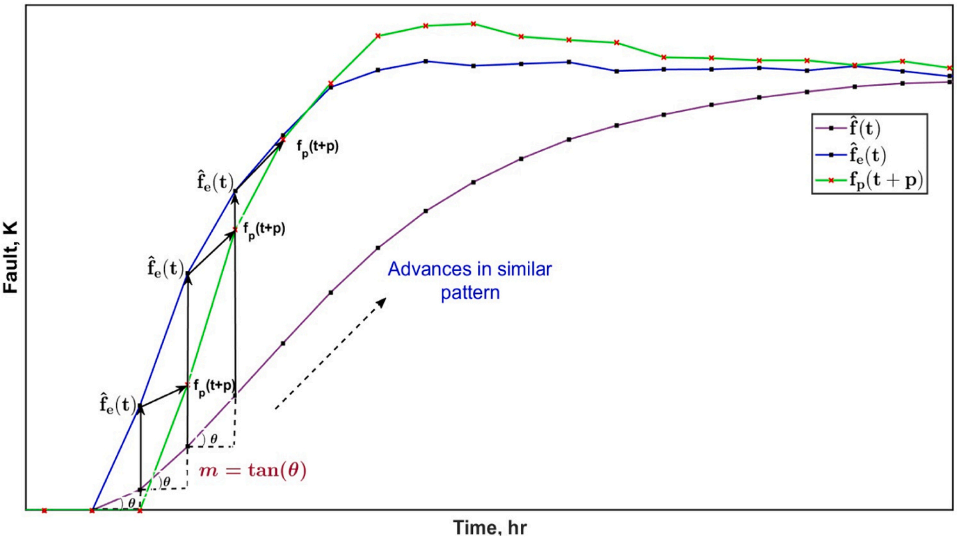

Fig. 8. Fault prediction scheme.

A very important parameter in the critical fault function is its lower bound: $f_{nc} = \inf_{t>0} f_c(t)$.

f_{nc} is the maximum fault size for which the state trajectory under nominal controller touches the SOS boundary but does not cross it. When $f < f_{nc}$, there is no need to activate the backup controller as it will be effectively handled by nominal controller, which will keep the system within SOS.

5. Proposed FTC strategy

In this section, an active FTC strategy is proposed capable of providing more accurate and timely information for decision-making and maintaining system functionality in the presence of faults. The FTC structure comprises three components as shown in Fig. 7, (i) fault estimation via functional observer (ii) fault prediction (iii) decision logic for activating the backup controller (BC).

The functional observer component has been discussed in subsection 3.1. In the present section the following will be derived: 1. the fault prediction algorithm, based on the fault estimate from the functional observer; 2. the decision logic for activating the backup controller. Also, the properties of the closed loop system under the proposed FTC algorithm as well as tuning issues are discussed.

5.1. Fault prediction

The basis for fault prediction will be a linear first order functional observer with tuneable eigen value (α_1), that generates a fault estimate $\widehat{f}$, following subsection 3.1. From (13), the rate of change of estimated fault follows:

$$\frac{d\widehat{f}}{dt} = -\alpha_1\widehat{f} + \beta_1 x + \beta_0\frac{dx}{dt} \tag{28}$$

But because β_0 and β_1 satisfy (12), this implies that

$$\frac{d\widehat{f}}{dt} = -\alpha_1\widehat{f} + \mathrm{M}(\mathrm{R} + \alpha_1 I)x_o \tag{29}$$

For the case of a step fault ($\mathrm{M} = 1, \mathrm{R} = 0$), the fault estimate is related to the actual fault according to:

$$\frac{d\widehat{f}}{dt} + \alpha_1\widehat{f} = \alpha_1 f \tag{30}$$

From (30), it is evident that if the rate of change of the fault $(\widehat{\frac{df}{dt}})$ can be estimated from the online data of $\widehat{f}(t)$ from the functional observer over a small time interval, an improved fault estimate may be derived as: $(\frac{1}{\alpha_1}\frac{d\widehat{f}}{dt} + \widehat{f})$. This is based on the assumption that the fault follows a nearly constant slope during this time interval. The time derivative $\left(\widehat{\frac{df}{dt}}\right)$ may be estimated through linear regression (LR) on the on line $\widehat{f}$ data over a pre-defined time interval $[t - t_s, t]$ of length t_s, and then a projected fault estimate $(\widehat{f}_e(t))$ can be derived:

$$\widehat{f}_e(t) = \widehat{f}(t) + \frac{m(t)}{\alpha_1} \tag{31}$$

where, $m(t) = \left(\widehat{\frac{df}{dt}}\right)_{LR}$ is the estimated rate of change of fault through LR. The above projected estimate corrects for the lag between estimated and actual faults, making $\widehat{f}_e(t)$ closer to the actual fault. Moreover, (30) may be used to extrapolate the fault estimate into the future, as follows.

If p is a small enough time horizon, such that the time derivative $(\widehat{\frac{df}{dt}})$ remains approximately constant over the time interval $[t, t+p]$, (30) implies that the change in f will be approximately equal to the change in $\widehat{f}$:

$$f(t+p) - f(t) \approx \widehat{f}(t+p) - \widehat{f}(t) \approx \left(\frac{d\widehat{f}}{dt}\right)_{approx} \bullet p \tag{32}$$

The above approximation allows to predict $f(t+p)$ considering $\widehat{f}_e(t)$ to be an accurate estimate of $f(t)$ and using the estimate $m(t) = \left(\widehat{\frac{df}{dt}}\right)_{LR}$ obtained through LR as an approximation of the derivative, as follows:

$$f_p(t+p) = \widehat{f}_e(t+p) = \widehat{f}_e(t) + m(t)p \tag{33}$$

Fig. 8 shows the fault prediction scheme with estimated fault and its rate of change.

5.2. Decision logic for activating the backup controller

The decision logic involves real-time actions guided by the results of offline calculations. The offline calculations as discussed in Section 4 include computation of:

(a) A predefined set Φ, the Safe Operating Set (SOS), that reflects the capabilities of the backup controller over the entire range of

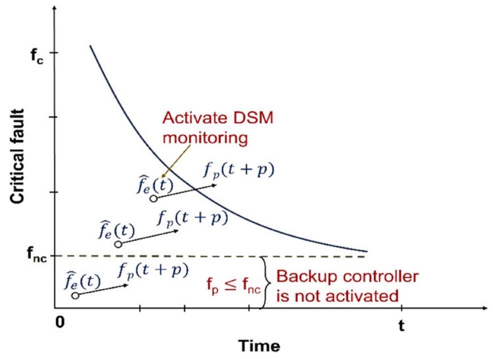

Fig. 9. Decision logic for activating DSM monitoring in continuous-time.

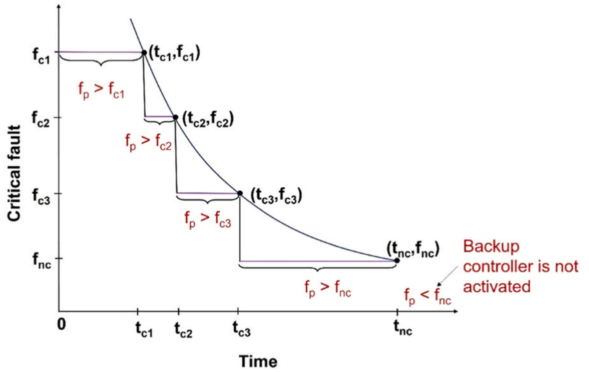

Fig. 10. Decision logic for activating DSM monitoring in discrete-time. Remark: In the above, it was assumed, without loss of generality, that the fault occurred at time $t = 0$. The time of occurrence of the fault t_o is determined by the estimate from the functional observer, and the elements of the t_c sequence must be shifted to $t_c + t_o$.

possible fault sizes (see subsection 4.1). The algorithm will involve real-time monitoring of the Dynamic Safety Margin (DSM), which is the distance from the boundary of Φ, to decide when the backup controller will be activated.

(b) A precalculated function $f_c(t)$, the Critical Fault Function (CFF), that will define the time-dependent threshold for initiating real-time monitoring of the DSM.

To set up a criterion for activating DSM monitoring and subsequently the backup controller, consider a fault constant size $f > 0$, occurring at $t = 0$, under only the nominal controller operating. Then, it is known that the safety constraints will be violated after time $t_c = f_c^{-1}(f)$. Therefore, activation of the backup controller must occur before the above tine t_c so that trajectory cannot go outside of SOS:

$$t_{activation} \quad < \quad f_c^{-1}(f) \tag{34}$$

or equivalently

$$f_c(t_{activation}) \quad < \quad f \tag{35}$$

If the projected, lag-corrected fault estimate $\widehat{f_e}(t)$ is used and action is taken at time t when $\widehat{f_e}(t) = f_c(t)$, it could be too late. To be able to act cautiously and ahead of time, the fault prediction $f_p(t+p)$, over a prediction horizon $p > 0$, is used and to get alert and initiate real-time monitoring of the DSM, at the first-time instant t such that

$$f_p(t+p) > f_c(t) \tag{36}$$

Because of the positivity of the fault f, the estimate $\widehat{f}(t)$ from the linear first-order functional observer will be an increasing function of time and therefore $f_p(t+p)$ will be larger than f, and this guarantees that action is taken ahead of time, before the system trajectory crosses SOS boundary. The prediction horizon p is a robustness parameter in the FTC scheme. Fig. 9 depicts the application of criterion (36): when the predicted fault $f_p(t+p)$ exceeds the critical fault $f_c(t)$, DSM monitoring is activated at that moment. The backup controller is activated if and when DSM $\le \varepsilon$, where $\varepsilon > 0$ is a tunable parameter, which represents a robustness margin.

Note that in general, it is not possible to do an analytical calculation of the function $f_c(t)$ or $t_c = f_c^{-1}(f)$. The best approach is to numerically calculate pairs (t_c, f_c), and thus generate a piecewise approximation of the function:

$$f_c^{approx}(t) = \begin{cases} f_{c1}, & if \ \ 0 < t \le t_{c1} \\ f_{c2}, & if \ \ t_{c1} < t \le t_{c2} \\ f_{c3}, & if \ \ t_{c2} < t \le t_{c3} \\ \vdots & \\ f_{cn}, & if \ \ t_{c(n-1)} < t \le t_{cn} \end{cases} \tag{37}$$

the understanding being that a reasonable number of points (t_c, f_c) have been calculated, sufficiently close to each other, for accuracy. The approximation has the property that $f_c^{approx}(t) \le f_c(t)\ \forall t > 0$, therefore it provides a conservative estimate: if DSM monitoring is initiated once $f_p(t+p) > f_c^{approx}(t)$, this will happen earlier than the time when $f_p(t+p) > f_c(t)$. Thus, the discretized decision logic will be:

$$f_p(t+p) > f_c^{approx}(t) \tag{38}$$

$$f_p(t+p) > f_{cn}(t_{cn}), \forall \quad t \quad \in \{t_{c(n-1)}, \quad t_{cn}\}$$

and it will be effective in ensuring in-time action. The discretization of $f_c(t)$ and the discretized logic are illustrated in Fig. 10. Condition (38) ensures that the decision to take action is made within the time interval between the previous critical time $t_{c(n-1)}$ and the current critical time t_{cn}. If the predicted fault surpasses the critical fault size within this interval, corrective action needs to be initiated to maintain system safety. In this formulation, the decision logic provides a clear criterion for activating fault-tolerant measures based on the comparison between predicted and critical fault sizes within the specified time window. Thus, the FTC algorithm keep the system within SOS in the presence of fault by activating BC in timely manner.

5.3. Properties of the FTC control system – Tuning considerations

The proposed FTC algorithm detailed in the previous subsections was built in such a way, so that it does not let the system state escape out of the set Φ. In particular, one can prove the following:

Proposition: Suppose that the following assumptions are satisfied:

(A1) The fault is initially zero and then it undergoes an ideal step increase to the value of $f \in [0, f_{\max}]$;

(A2) Full state measurement without noise or systematic error;

(A3) The functional observer is linear and first-order;

(A4) The set Φ is a positively invariant closed set, for the closed-loop system under NC+BC*, for every constant $f \in [0, f_{\max}]$; the design steady state lies in the interior of the set Φ;*

(A5) The function $f_c(t)$ is a monotonically decreasing continuous function such that for every constant $f \in [0, f_{\max}]$, the inverse function $t_c = f_c^{-1}(f)$ represents the time it takes, after the occurrence of a fault f, for the closed loop system under NC *to cross the boundary of Φ;*

(A6) The set Φ is a subset of the DSS of the closed-loop system under NC *alone, for all $f \in [0, \inf_{t>0} f_c(t)]$;*

Then the FTC algorithm guarantees that the state of the system lies in the set Φ for all $t > 0$.

Proof: The functional observer will generate a fault estimate that follows (30), hence for a step fault f, the estimate will be $\widehat{f}(t) = (1 - e^{-\alpha_1 t})f$, which is a strictly increasing positive function, from which

Table 1
Process parameters.

Parameter description	Symbol	Value	Unit
Pre-exponential factor	k_{10}	4×10^{14}	lit/mol hr
Pre-exponential factor	k_{20}	1×10^{84}	hr^{-1}
Activation energy	E_1	1.28×10^5	J/mol
Activation energy	E_2	8×10^5	J/mol
Heat of reaction	ΔH_1	−45400	J/mol
Heat of reaction	ΔH_2	-3.2×10^5	J/mol
Universal gas constant	R	8.314	J/mol K
Average density of feed	ρ	12.4	mol/lit
Average specific heat of feed	C_p	254	J/mol K
Volume of reactor	V	5000	lit
Flowrate of A	F_{A0}	1250	mol/hr
Flowrate of S	F_{S0}	750	mol/hr
Flowrate of B	F_{B0}	1400	mol/hr
Coolant temperature	T_c	300	K
Heat transfer surface area	A	5.3	m^2
Overall heat transfer coefficient	U_s	11000	J/ m^2 hr K
Reactor temperature	T_s	468	K
Concentration of A	C_{As}	0.16	mol/lit
Feed temperature	T_0	416	K
Total feed volumetric flowrate	$V_{0\ s}$	274.2	lit/hr

Note that in the vicinity of normal operating conditions, with the reactor temperature below 480 K, the side reaction does not go and the process model is reduced to a two-state model as: $\frac{dC_A}{dt} = \frac{V_0}{V}(C_{A0} - C_A) - R_1(C_A, T)$ and $\frac{dT}{dt} = \frac{V_0}{V}(T_0 - T) - \frac{UA(T - T_c)}{\rho V C_p} + \frac{(-\Delta H_1)R_1(C_A, T)}{\rho C_p}$.

the prediction is $f_p(t+p) = \widehat{f}_e(t) + p\widehat{\frac{df}{dt}}(t) = (1+p\alpha_1 e^{-\alpha_1 t})f$.

Because $\alpha_1 > 0$ and $p > 0$, the prediction $f_p(t+p) > f$ for all $t > 0$, therefore if there is an intersection of $f_p(t+p)$ with $f_c(t)$, it will be at time less than $t_c = f_c^{-1}(f)$, i.e. while the system state lies in the interior of Φ. From that moment, DSM monitoring will start, and the BC will be activated when DSM reaches the value $\varepsilon > 0$, i.e. while the system is still in the interior of Φ. And it will remain in Φ in subsequent times under the action of BC+NC.

On the other hand, if there is no intersection of $f_p(t+p)$ with $f_c(t)$, this means that the system state lies in the interior of Φ. □

Of course, there will be non-idealities in practice, including sensor noise, non-ideal step fault, errors in estimating the time derivative of the fault estimate, errors in calculating f_c, etc., however the FTC algorithm has two robustness parameters, p and ε, that may be appropriately tuned to cover for these errors.

The FTC algorithm has the following tunable parameters that need to be properly selected:

Table 2
Controller parameters.

Controller Parameter	Value	Unit
k_1	-10^6	J lit/ m^2 hr K mol
k_2	-7×10^6	J / m^2 hr K^2
l_1	−100	lit^2/mol hr
l_2	60	lit/ hr K
U_{max}	25000	J/ m^2 hr K
V_{0max}	1.5×v0s	lit/hr
U_{min}	0	J/ m^2 hr K
$V_{0\ min}$	0	lit/hr

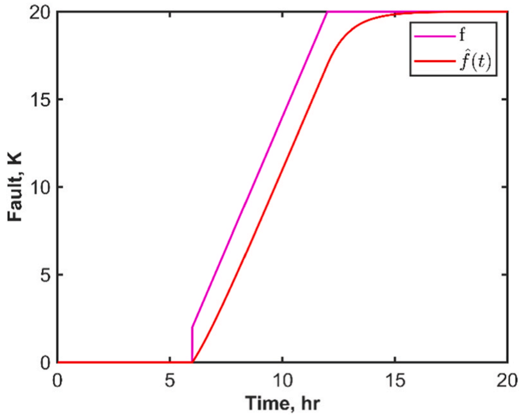

Fig. 12. Fault estimation in open loop.

- *Eigenvalue of the functional observer*: It must be selected to strike a balance between the convergence speed of the estimator and minimizing the impact of noise on overshoot.
- *Sampling interval for linear regression*: It represents a fraction of the time constant and should be shorter than the prediction horizon.
- *Prediction horizon*: This parameter should be small enough to prevent over-reaction, but at the same time large enough to cover for possible calculation errors in the critical faults.
- *DSM threshold:* It should be set small enough to prevent unnecessary activation of backup controller, but large enough to cover for modelling error.

Table 3
Steady state at upper and lower limit of input.

State	U_{max}	U_{min}
T_s	453 K	759.6 K
C_{As}	0.36mol/lit	0mol/lit

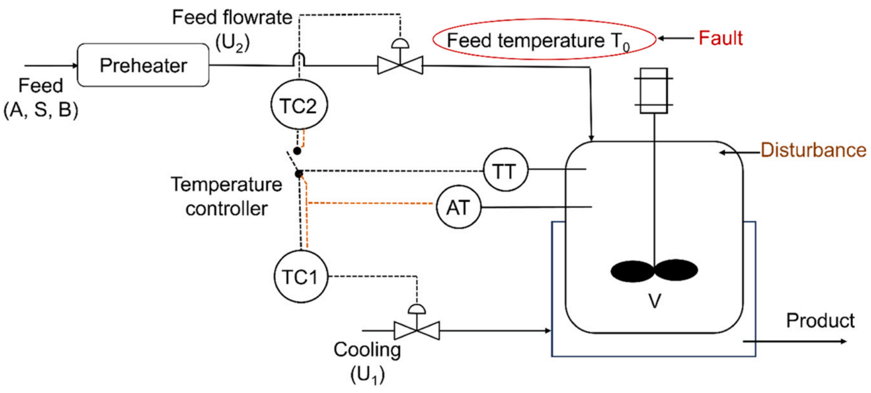

Fig. 11. T2-process schematic.

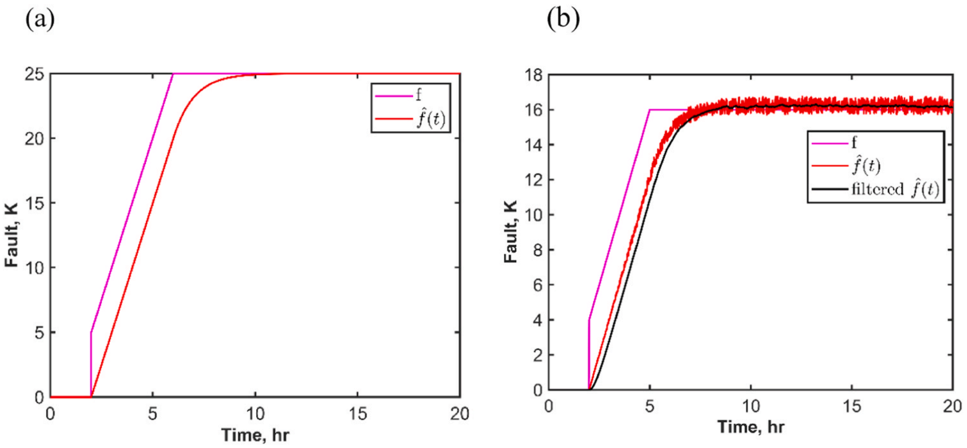

Fig. 13. Response of functional observer in closed loop under input constraints (a) without noise (b) with noise in measurement.

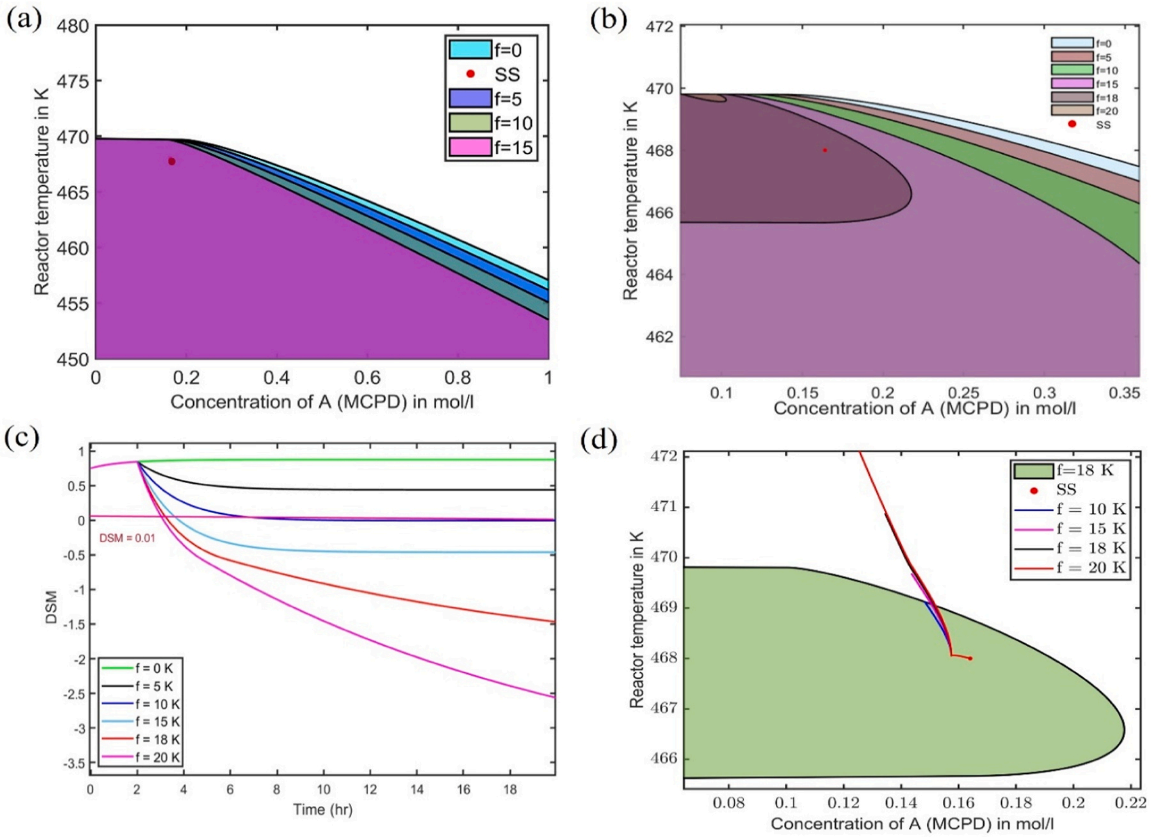

Fig. 14. DSS under NC, (b). DSS of combined NC+ BC, (c). DSM for different fault sizes under NC, (d). Trajectory under NC.

Table 4
Pairs of critical fault, f_c and critical time, t_c.

n	f_c (K)	t_c (hr)
1	20	1.1
2	18	1.2
3	15	1.75
4	10	6.5 (to touch the boundary)
5	5	Does not cross the DSS
6	0	Does not cross the DSS

Offline computation of SOS and t_c are based on an ideal step fault, providing a conservative estimate of the time left for crossing the SOS without activating BC. The fault estimation scheme closely resembles the actual fault size and the prediction horizon in the decision logic provides early fault identification that guide decision logic for activating DSM monitoring. The positive threshold value for DSM to activate backup controller, serves as a real-time indicator of the system’s safety level implying that the system is well within the SOS. These features ensure there is sufficient time to take corrective action for step and even for step- like faults.

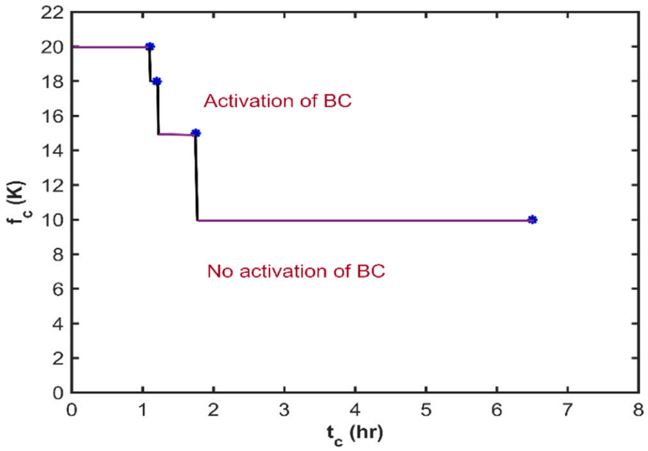

Fig. 15. Critical time / critical fault pairs (for fault occurrence time t_o =0).

Table 5
Tunable parameters.

Parameter	Value
α_1	1 hr
t_s	0.25 hr
p	0.25 hr
ε	0.01

6. Case study: fault-tolerant control of an exothermic chemical reactor

In what follows, a case study will be used to illustrate the proposed FTC strategy in terms of offline computation and real-time decision-making to keep system within SOS. It will involve designing the nominal (fault-free) and backup controller for maintaining the reactor temperature at a target set point. The backup controller will be activated only in the presence of faults of significance size. The reactions include one primary desired reaction and a secondary undesired reaction, both of which are exothermic. The undesired reaction has a reaction rate that is negligible under normal operating conditions but becomes significant at elevated temperatures. In other words, the undesirable side reaction can be triggered under transient conditions, when the reactor temperature is not maintained within safety limits. This aspect allows to elucidate the advantages of the proposed FTC strategy. The fault estimator and the necessary offline computations for the design of FTC scheme will be derived in this section.

6.1. Process description

The process is the T2 Laboratories production of Methyl-Cyclopentadienyl Manganese Tri-carbonyl (MCMT) through two exothermic reactions, which take place in a CSTR [41]

Reaction 1: $A + B \longrightarrow^{K_{1A}} C + ½ D$

Reaction 2: $S \longrightarrow^{K_{2S}} 3D + byproducts$

where A (methylcyclopentadiene), B (liquid sodium) are the reactants, C (sodium methylcyclopentadiene) is the desired product, S (diglyme) is the solvent, and D is hydrogen. Reaction 2, identified as the side reaction, has a negligible rate at temperatures below 480 K. However, it becomes significant above 480 K due to its activation energy being over eight times greater than that of the desired main reaction. Consequently, this leads to an uncontrolled increase in reaction rate at elevated temperatures. Given that both reactions produce hydrogen gas, there is a potential for a sharp increase in pressure, that can result in the rupture of the reactor wall. Hence, it is imperative to enforce the safety constraint of reactor temperature below 480 K, to prevent thermal runaway. The open loop dynamic model considering mass and energy balance in the absence of faults and disturbances are:

Table 6
Decision logic for activating DSM monitoring.

Condition	Time interval (hr)
$f_p(t+p) > 20$	$2 < t \leq 3.1$
$f_p(t+p) > 18$	$3.1 < t \leq 3.2$
$f_p(t+p) > 15$	$3.2 < t \leq 3.75$
$f_p(t+p) > 10$	$3.75 < t \leq 8.5$

$$\frac{dC_A}{dt} = \frac{V_0}{V}(C_{A0} - C_A) - R_1(C_A, T) \tag{39}$$

$$\frac{dC_S}{dt} = \frac{V_0}{V}(C_{S0} - C_S) - R_2(C_s, T)$$

$$\frac{dT}{dt} = \frac{V_0}{V}(T_0 - T) - \frac{UA(T - T_c)}{\rho V C_p} + \frac{(-\Delta H_1)R_1(C_A, T) + (-\Delta H_2)R_2(C_s, T)}{\rho C_p}$$

where cooling duty, Q, can be represented by: $UA(T - T_c)$

The reaction rates of the two reactions are given by [50]:

$$R_1(C_A, T) = k_{10}e^{-\frac{E1}{RT}}C_A(C_A + C_{B0} - C_{A0}) \tag{40}$$

$$R_2(C_s, T) = k_{20} \quad e^{-\frac{E2}{RT}}C_S$$

The process parameter is given in Table 1 where subscript lower-case s refers to their steady state.

The feed streams reactant (A) in solvent (S) and liquid (B), are heated in a preheater before being fed to the reactor as shown in Fig. 11. The process has full state measurement for monitoring. A static state feedback controller is designed to ensure efficient real-time control with minimal computational complexity. This approach is particularly suited for the proposed FTC algorithm, allowing for rapid fault estimation and reconfiguration without relying on internal dynamics or integrators. Although techniques like bumpless transfer or anti-windup could further smooth transitions, the static feedback design effectively handles system stability under fault conditions. The reactor temperature is controlled at the desired set-point using a nominal state feedback controller manipulating the heat transfer coefficient by adjusting the flowrate of the cooling water; this is the only controller to operate in the absence of faults. Additionally, a backup state feedback controller manipulating feed flowrate is designed to operate when fault happens. Thus, a nominal controller is capable of handling disturbances and small fault size, and a backup controller capable of handling large fault sizes. Table 2 shows the controller gain parameters: feedback gains and input saturation limits. The controller equations are given by (41) below:

$$Q_s = U_s A(T_s - T_c) \tag{41}$$

$$Q = -k_1(C_A - C_{As}) - k_2(T - T_s) + Q_s$$

$$U = \max(U_{\min}, \min(\left(\frac{-k_1(C_A - C_{As}) - k_2(T - T_s) + Q_s}{A(T - Tc)}\right), U_{\max}))$$

$$V_0 = \max(V_{0\min}, \min((-l_1(C_A - C_{AS}) - l_2(T - T_s) + V_{0s}), V_{0\max}))$$

6.2. Fault estimation

The functional observer algorithm is applied for fault estimation described in subsection 3.2, using the two-state model, with the equations expressed in deviation form in terms of $C_A' = C_A - C_{As}$, $T' = T - T_s$, $Q' = Q - Q_s$. The process fault considered is overheating in the feed

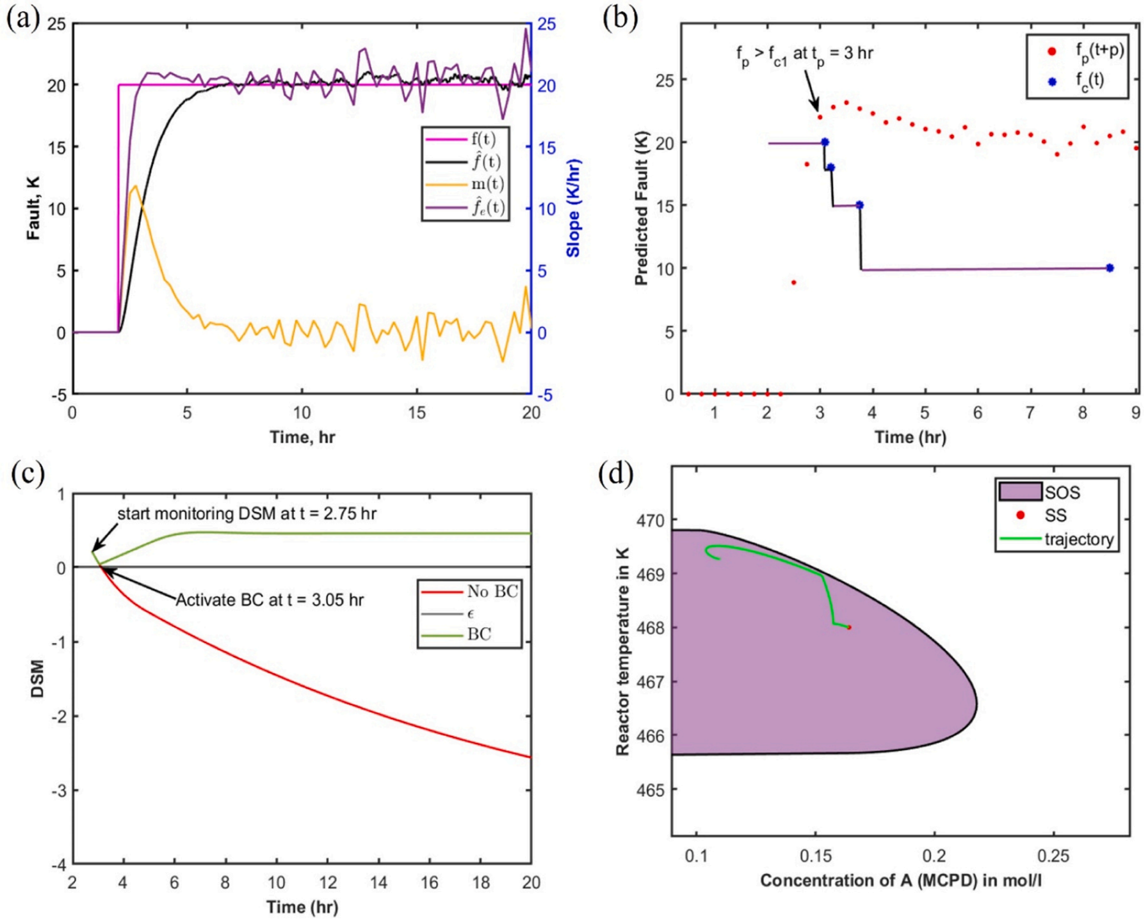

Fig. 16. (a). Fault estimation, (b). Predicted fault, (c). DSM response, (d). Trajectory with activating BC at 3.05 hr for step fault.

pre-heater, which directly impacts fault (f) in feed temperature (f is the deviation of feed temperature from its normal value), also a disturbance of size w = 0.05 is considered. Thus, the open-loop model in deviation form is given by (42).

$$\frac{dC_A'}{dt} = \frac{-V_0}{V}C_A' + (1+w)(R_1(C_{As},T_s) - R_1(C_A' + C_{As}, T' + T_s)) \tag{42}$$

$$\frac{dT'}{dt} = \frac{V_0}{V}(-T' + f) + \frac{(-\Delta H_1)(1+w)(R_1(C_A' + C_{As}, T' + T_s) - R_1(C_{As},T_s))}{\rho C_p} - \frac{Q'}{\rho V C_p}$$

$$y_1' = C_A'$$

$$y_2' = T'$$

The following parity vectors satisfy the conditions of (7–9) for v = 1 in open loop, where Q' = 0.

$$\beta_0 = \alpha_1 \frac{V}{V_0}\left[\frac{-\Delta H_1}{\rho C_p} \quad , \quad 1\right] \tag{43}$$

$$\beta_1 = \alpha_1\left[\frac{-\Delta H_1}{\rho C_p} \quad , \quad 1\right]$$

The linear functional observer along with the pertinent design parameters in open loop are:

$$\mathrm{A} = -\alpha_1 = -1, \mathrm{B} = \beta_1 - \alpha_1\beta_0, \mathrm{C} = 1, \mathrm{D} = \beta_0, \alpha_1 = 1 \tag{44}$$

$$\frac{d\hat{\xi}}{dt} = -\alpha_1\hat{\xi} + \alpha_1\frac{-\Delta H_1}{\rho C_p}\left(1 - \alpha_1\frac{V}{V_0}\right)y_1' + \alpha_1(1 - \alpha_1\frac{V}{V_0})y_2'$$

$$\hat{f} = \hat{\xi} + \alpha_1\frac{V}{V_0}\frac{(-\Delta H_1)}{\rho C_p}y_1' + \alpha_1\frac{V}{V_0}y_2'$$

The following step-like fault scenario was simulated and the result is shown in Fig. 12.

$$f(\mathrm{t}) = \begin{cases} 0, & t < 6 \\ 3t - 16, & t \geq 6 \\ 20, & t \geq 12 \end{cases} \tag{45}$$

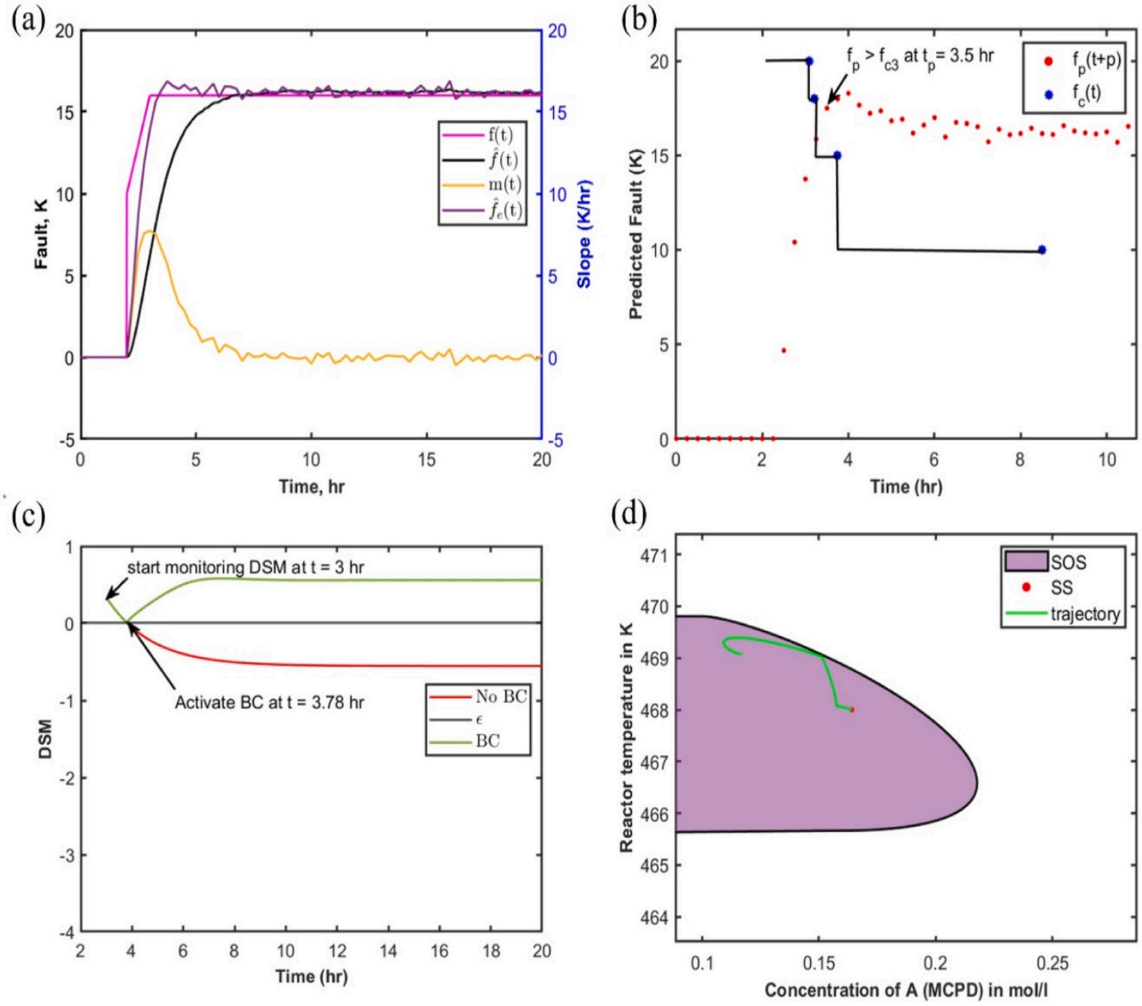

Fig. 17. (a). Fault estimation, (b). Predicted fault, (c). DSM response, (d). Trajectory with activating BC at 3.78 hr for fault given by (50).

The following parity vectors satisfy the conditions of (7−9) for $v = 1$ in closed loop $Q' = -k_1 C_A' - k_2 T'$ and the functional observer equations are:

$$\beta_0 = \quad \alpha_1 \frac{V}{V_0}\left[\frac{-\Delta H_1}{\rho C_p}, \quad 1\right] \tag{46}$$

$$\beta_1 = \quad \alpha_1 \left[\frac{-\Delta H_1}{\rho C_p} - \frac{k_1}{\rho C_p V_0}, \quad 1 - \frac{k_2}{\rho C_p V_0}\right]$$

$$\frac{d\widehat{\xi}}{dt} = -\alpha_1 \widehat{\xi} + \alpha_1 \frac{(-\Delta H_1)}{\rho C_p}\left(1 - \frac{k_1}{(-\Delta H_1)V_0} - \alpha_1 \frac{V}{V_0}\right) y_1' + \alpha_1 (1 - \frac{k_2}{\rho C_p V_0} - \alpha_1 \frac{V}{V_0}) y_2'$$

$$\widehat{f} = \widehat{\xi} + \alpha_1 \frac{V}{V_0}\frac{(-\Delta H_1)}{\rho C_p} y_1' + \alpha_1 \frac{V}{V_0} y_2'$$

The above equations are used when the manipulated input does not saturate. At the moment it saturates to $U_{\max}$ or $U_{\min}$, switch to the corresponding open-loop Eq. (44), but with new steady-state values corresponding to the respective limiting of input given in Table 3.

The fault scenario (48) was simulated and the response is shown in Fig. 13 (a). Also, the response of the functional observer in the presence of measurement noise (47) for the fault scenario (49) is shown in Fig. 13 (b). The simulation results indicate that the functional observer's performance is excellent in the presence of any fault size in closed loop, considering input constraints and noise.

$$y_1' = \quad C_A' + 0.03 C_A' r$$

$$y_2' = \quad T' + 0.03 T' r \tag{47}$$

where, r is the random number from uniform distribution in the interval (0,1). Fast Fourier transform is used for noise filtering in estimating fault. The FFT is fast and efficient in noise filtering for large noisy data sets.

$$f(t) = \begin{cases} 0, & t < 2 \\ 5t - 5, & t \geq 2 \\ 25, & t \geq 6 \end{cases} \tag{48}$$

$$f(t) = \begin{cases} 0, & t < 2 \\ 4t - 4, & t \geq 2 \\ 16, & t \geq 5 \end{cases} \tag{49}$$

6.3. Offline calculations for the FTC algorithm

As discussed in Section 4, it is necessary to determine the SOS and the (t_c, f_c) pairs offline, to implement the FTC strategy. The results of the calculations of DSS as discussed in subsection 3.2 for different fault sizes under (a) nominal controller alone (b) combined nominal and backup controllers are shown in Fig. 14(a) and (b) respectively. Under NC alone, the size of the DSS decreases with increasing fault size and becomes empty for faults exceeding 15 K. whereas under combined NC + BC, the

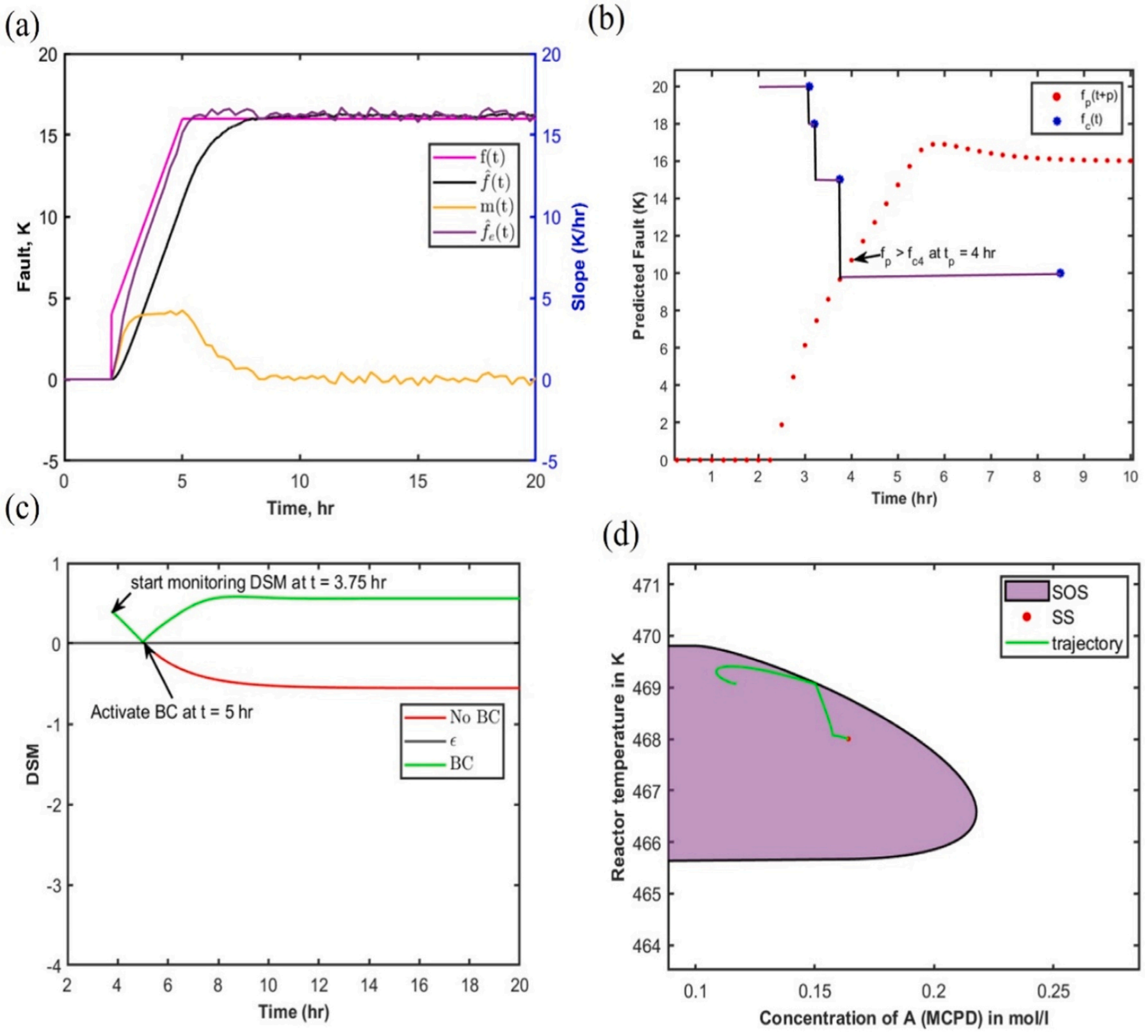

Fig. 18. (a). Fault estimation, (b). Predicted fault, (c). DSM response, (d). Trajectory with activating BC at 5 hr for fault given by (51).

DSS exists and becomes extremely small for fault exceeding 18 K. For the FTC algorithm, the DSS corresponding to fault of 18 K under both controllers is selected, as the SOS (the set Φ) which has reasonable size. This set will be used for critical fault calculations and for online DSM monitoring. It turns out that the calculated approximation of DSS is an underestimation, and it is adequate to manage faults greater than 18 K, keeping the system below the upper boundary of DSS (which is approximately constant for different fault sizes, as shown in Fig. 14. (b)).

The critical time t_c to cross the boundary of the SOS for different step fault sizes is calculated by identifying time when trajectory touches the safety boundary, making DSM equal to zero. Fig. 14 (c) shows DSM decreases down to zero for fault size of 10 K but dips into negative values for larger fault sizes. In this case, fault size of 10 K is the f_{nc} below which the backup controller is not needed (see subsection 4.2). As DSM becomes negative for faults greater than 10 K, trajectory crosses the SOS as shown in Fig. 14.(d), if the backup controller is not activated. Thus, take corrective actions for faults greater than 10 K. Table 4 provides some (t_c, f_c) pairs, considering the fault occurrence time, t_o to be zero. The corresponding discretized critical fault function is depicted in Fig. 15 showing how critical time decreases with increasing fault size, indicating a reduced window for intervention as faults escalate. Finally, the tunable parameters used in the FTC algorithm for fault estimation, projection, prediction and DSM tolerance are listed in Table 5.

7. Results

In the previous section, the linear functional observer is derived for estimating fault size and the offline calculation results, including SOS and the discretized critical fault function. Now, the decision logic will be developed to implement the FTC scheme in real time. In this section, four sets of simulation results are provided for ideal step and step-like faults of different sizes given by (50–52). The time of occurrence of fault (t_o) is 2 hr in the simulations and therefore the critical time shown in Table 4 has been shifted to ($t_c + 2$) hr in the formulation of decision logic shown in Table 6. Thus, the offline (t_c, f_c) pairs and decision logic give conditions to check for the predicted fault for different time intervals, as shown in Table 6.

Fig. 16 illustrates the first scenario, when an ideal step fault of size 20 K occurs at t=2 hr. Firstly, the fault estimate is calculated from the functional observer and then linear regression is performed on 15 min data to calculate the rate of change of fault estimate (m). The projected fault closely resembles the real fault with minimal overshoot and noise indicating tunable parameters are well chosen. When current time t=2.75 hr and predicted fault at t=3 hr is larger than 20 K, the decision logic dictates to start monitoring DSM. Therefore, monitoring DSM starts at 2.75 hr and the backup controller is activated at t= 3.05 hr when DSM reaches its threshold. Fig. 16(d) shows that trajectory remains inside SOS for all times, indicating accommodation of the fault.

The next scenario is a step-like fault given by (50), involving an

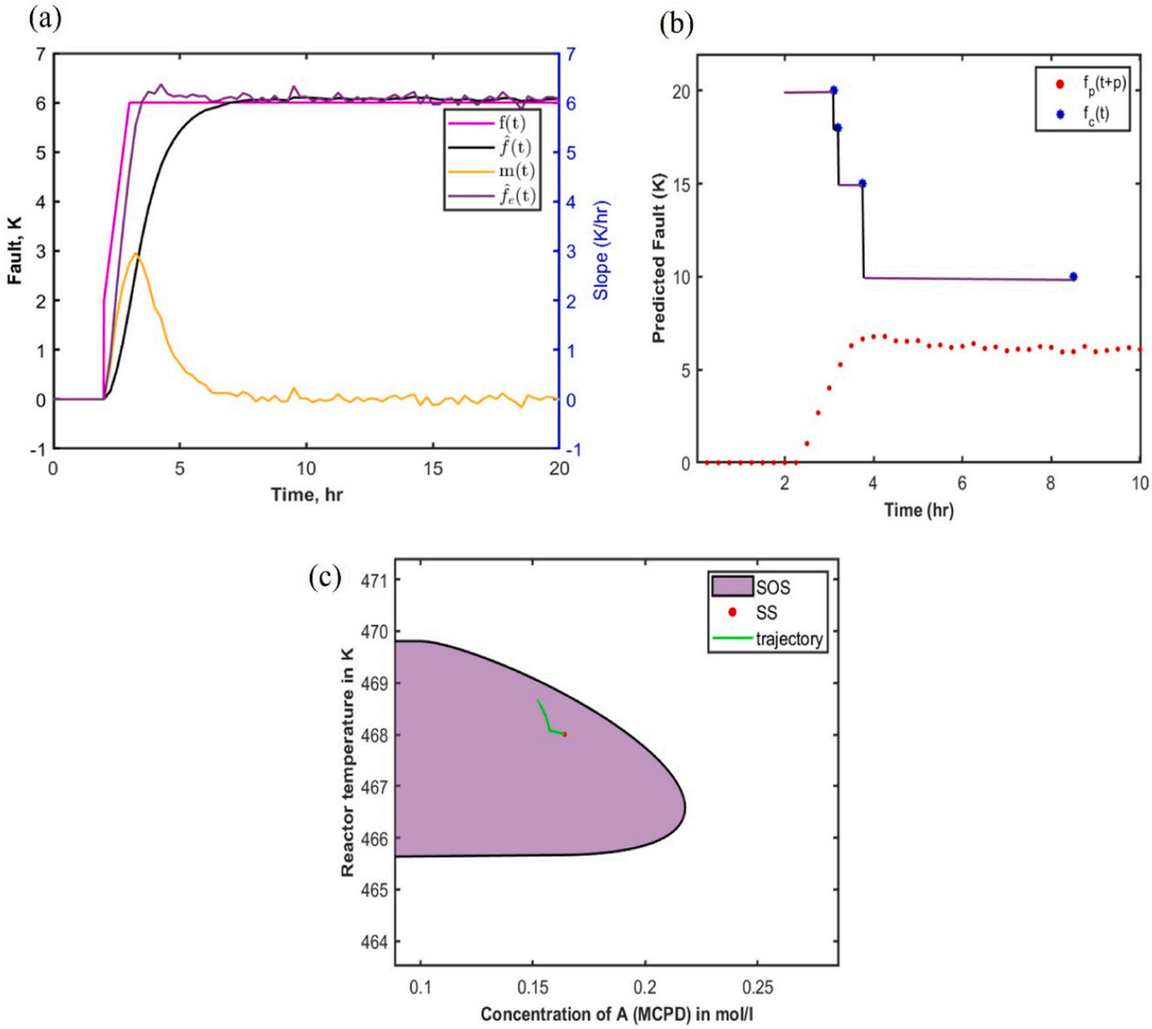

Fig. 19. (a). Fault estimation, (b). Predicted fault, (c). Trajectory without activating BC for fault given by (52).

initial growth phase and settling at its final value at a time close to t_{c1}. Again, linear regression is performed on 15 min data of fault estimate to calculate the rate of change of fault estimate (m). Here, the predicted fault is less than $f_{c1}(20\text{ K})$ and $f_{c2}(18\quad K)$ in their respective time interval. However, at current time t=3.25 hr, the predicted fault at t=3.5 hr, is greater than $f_{c3}\quad(15\text{K})$, which satisfies the condition of the decision logic. So, start monitoring the DSM at t=3.25 hr, and activate the backup controller at t=3.78 hr according to the DSM threshold value, to keep trajectory within SOS as shown in Fig. 17(d). Similarly, Fig. 18 shows the results for the step-like fault scenario given by (51), where the settling time is larger than t_{c1}. The predicted fault at t=3 is 6.22 K that can be handled by nominal controller. This indicates although the fault has occurred but its rate of change is slow. Here, the predicted fault is less than $f_{c1}(20\text{ K})$, $f_{c2}(18\quad K)$ and $f_{c3}(15\quad K)$ for their respective time interval. However, at current time t=3.75 hr and predicted fault at t=4 hr, is greater than $f_{c4}(10\text{K})$ which crosses the CFF as shown in Fig. 18(b). So, start monitoring the DSM at t=3.75 hr, and activate backup controller at t=5 hr according to DSM threshold to keep trajectory within SOS as shown in Fig. 18(d).

The last scenario simulated involves a small-size step-like fault given by (52), as shown in Fig. 19. Here, the predicted fault is always less than $f_{nc}(10K)$ that results in no activation of backup controller. This fault size is handled by nominal controller to keep the system within SOS as shown in Fig. 19(c).

In all cases, the algorithm is able to handle the faults and keep system within SOS. When the rate of change of fault is slow, although the DSM monitoring is activated early, the backup controller is only engaged just-in-time due to the two levels of safety embedded in the algorithm. The scheme involves first activating DSM monitoring, and then, when the DSM threshold is reached, the backup controller is triggered. This feature makes the proposed FTC algorithm effective for a wide range of fault scenarios.

$$f(t) = \begin{cases} 0, & t < 2 \\ 6t - 2, & t \geq 2 \\ 16, & t \geq 3 \end{cases} \tag{50}$$

$$f(t) = \begin{cases} 0, & t < 2 \\ 4t - 4, & t \geq 2 \\ 16, & t \geq 5 \end{cases} \tag{51}$$

$$f(t) = \begin{cases} 0, & t < 2 \\ 4t - 6, & t \geq 2 \\ 6, & t \geq 3 \end{cases} \tag{52}$$

8. Conclusions and future directions

In this work, a comprehensive framework for fault-tolerant control systems (FTCS) in the context of modern industrial processes characterized by nonlinear and multivariable interactions is proposed. Unlike existing methods for FTC schemes in the literature that rely on Fault Detection and Isolation (FDI) and Lyapunov-based methods for controller reconfiguration, our proposed method simplifies the process by focusing on maintaining system stability within a single SOS using information from fault estimator. The proposed approach integrates a dynamic safe set (DSS) and dynamic safety margin (DSM) concepts with fault estimation techniques to provide a robust FTCS that ensures system stability and safety in the presence of faults. A linear functional observer to estimate the fault is combined with a fault prediction scheme to predict the fault size. This helps in early identification of fault, so that a fault estimator in transient can be utilized and apply switching logic for controller accommodation, before it is too late. The formulation of decision logic to activate a backup controller just-in-time to accommodate the fault, is the key contribution of this paper.

The DSS is based on the theoretical concept of maximal output admissible set which is a collection of all initial states for which the output satisfies safety constraints at all times, even in the presence of faults and disturbances. It helps to determine a Safe Operating Set (SOS), which is the intersection of DSS over a range of different fault sizes. The SOS is a conservative estimate as it accounts for maximum step fault scenario. The SOS is the region within which the system can operate safely under combined nominal and backup controller actions. The SOS provides a critical boundary that guides the system's response to faults, ensuring that corrective actions are taken in a timely and appropriate manner.

A critical aspect of the proposed FTC scheme is the introduction of critical fault and critical time functions. The critical time is the time for state trajectory to cross SOS boundary in the presence of a step fault known as critical fault, under the nominal controller only. These functions are used to determine the timing for activating backup controllers, based on the predicted fault size. When the predicted fault size is larger than the critical fault, DSM is monitored. The DSM provides insight on the safeness level of system by real-time evaluation of safety margins from the boundary of SOS. The backup controller is activated when DSM crosses a positive threshold, in order to keep the process within SOS in the event of a fault. This approach helps in preventing unnecessary control actions while maintaining system safety and performance.

The application of the FTC algorithm to an exothermic CSTR, an example of a safety-critical process, illustrates its effectiveness in handling a fault due to overheating in the pre-heater of the feed stream, by activating a backup controller manipulating feed flowrate, which is cutting the fuel line for the exothermic reaction. The results highlight the FTC algorithm's ability to adaptively respond to faults, maintaining the system within the SOS and enforcing stability and safety constraints.

Future research will focus on extending this FTC scheme to other types of processes and fault scenarios, and refining the integration of DSS and DSM with various control strategies. Actuator and sensor faults will be considered in the FTC scheme. Key areas of improvement include improving fault identification techniques including error, and optimizing the decision-making criteria for controller reconfiguration. Our objective is to contribute to the ongoing development of more resilient and reliable industrial automation systems, capable of maintaining safety and efficiency in increasingly complex operational environments.

CRediT authorship contribution statement

Ritu Ranjan: Writing – original draft, Visualization, Software, Methodology, Conceptualization. **Costas Kravaris:** Writing – review & editing, Visualization, Supervision, Conceptualization.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

Financial assistance from the National Science Foundation through the grant CBET- 2133810 is gratefully acknowledged.

Data Availability

Data will be made available on request.

References

[1] D. Theilliol, Y.M. Zhang, J.C. Ponsart, Fault tolerant control system against actuator failures based on re-configuring reference input, *2009 Int. Conf. Adv. Comput. Tools Eng. Appl.* (Jul. 2009) 480–485, https://doi.org/10.1109/ACTEA.2009.5227904.

[2] M. Blanke, M. Staroswiecki, N.E. Wu, Concepts and methods in fault-tolerant control, *Proc. 2001 Am. Control Conf. (Cat. No. 01CH37148)* (Jun. 2001) 2606–2620 vol.4, https://doi.org/10.1109/ACC.2001.946264.

[3] P. Mhaskar, J. Liu, and P.D. Christofides, *Fault-Tolerant Process Control: Methods and Applications*. Springer Science & Business Media, 2012.

[4] Y. Zhang, J. Jiang, Bibliographical review on reconfigurable fault-tolerant control systems, Annu. Rev. Control 32 (2) (Dec. 2008) 229–252, https://doi.org/10.1016/j.arcontrol.2008.03.008.

[5] F. Guenab, P. Weber, D. Theilliol, Y.M. Zhang, Design of a fault tolerant control system incorporating reliability analysis and dynamic behaviour constraints, Int. J. Syst. Sci. 42 (1) (Jan. 2011) 219–233, https://doi.org/10.1080/00207720903513319.

[6] J. Jiang, X. Yu, Fault-tolerant control systems: a comparative study between active and passive approaches, Annu. Rev. Control 36 (1) (Apr. 2012) 60–72, https://doi.org/10.1016/j.arcontrol.2012.03.005.

[7] X. Yu, J. Jiang, A survey of fault-tolerant controllers based on safety-related issues, Annu. Rev. Control 39 (Jan. 2015) 46–57, https://doi.org/10.1016/j.arcontrol.2015.03.004.

[8] A.A. Amin, K.M. Hasan, A review of fault tolerant control systems: advancements and applications, Measurement 143 (Sep. 2019) 58–68, https://doi.org/10.1016/j.measurement.2019.04.083.

[9] A. Fekih, Fault diagnosis and Fault Tolerant Control design for aerospace systems: a bibliographical review, *2014 Am. Control Conf.* (Jun. 2014) 1286–1291, https://doi.org/10.1109/ACC.2014.6859271.

[10] A. Abbaspour, S. Mokhtari, A. Sargolzaei, K.K. Yen, A survey on active fault-tolerant control systems, Art. no. 9, Electronics 9 (9) (Sep. 2020), https://doi.org/10.3390/electronics9091513.

[11] V. Venkatasubramanian, R. Rengaswamy, K. Yin, S.N. Kavuri, A review of process fault detection and diagnosis: part I: Quantitative model-based methods, Comput. Chem. Eng. 27 (3) (Mar. 2003) 293–311, https://doi.org/10.1016/S0098-1354(02)00160-6.

[12] S.X. Ding, *Model-based Fault Diagnosis Techniques: Design Schemes, Algorithms, and Tools*. Springer Science & Business Media, 2008.

[13] P.M. Frank, Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy: a survey and some new results, Automatica 26 (3) (May 1990) 459–474, https://doi.org/10.1016/0005-1098(90)90018-D.

[14] P.M. Frank, X. Ding, Survey of robust residual generation and evaluation methods in observer-based fault detection systems, J. Process Control 7 (6) (Dec. 1997) 403–424, https://doi.org/10.1016/S0959-1524(97)00016-4.

[15] M. Darouach, Existence and design of functional observers for linear systems, IEEE Trans. Autom. Control 45 (5) (May 2000) 940–943, https://doi.org/10.1109/9.855556.

[16] K. Emami, T. Fernando, B. Nener, H. Trinh, Y. Zhang, A functional observer based fault detection technique for dynamical systems, J. Frankl. Inst. 352 (5) (May 2015) 2113–2128, https://doi.org/10.1016/j.jfranklin.2015.02.006.

[17] P.M. Frank, Advanced fault detection and isolation schemes using nonlinear and robust observers, Part 3, IFAC Proc. Vol. 20 (5) (Jul. 1987) 63–68, https://doi.org/10.1016/S1474-6670(17)55353-7.

[18] N. Kazantzis, C. Kravaris, Nonlinear observer design using Lyapunov's auxiliary theorem, Syst. Control Lett. 34 (5) (Jul. 1998) 241–247, https://doi.org/10.1016/S0167-6911(98)00017-6.

[19] S.A.A. Taqvi, H. Zabiri, L.D. Tufa, F. Uddin, S.A. Fatima, A.S. Maulud, A review on data-driven learning approaches for fault detection and diagnosis in chemical processes, *ChemBioEng Rev.* 8 (3) (2021) 239–259, https://doi.org/10.1002/cben.202000027.

[20] X. Bi, R. Qin, D. Wu, S. Zheng, J. Zhao, One step forward for smart chemical process fault detection and diagnosis, Comput. Chem. Eng. 164 (Aug. 2022) 107884, https://doi.org/10.1016/j.compchemeng.2022.107884.

[21] D.-L. Yu, T.K. Chang, D.-W. Yu, Fault tolerant control of multivariable processes using auto-tuning PID controller, IEEE Trans. Syst. Man Cybern. Part B Cybern. 35 (1) (Feb. 2005) 32–43, https://doi.org/10.1109/TSMCB.2004.839247.

[22] P. Mhaskar, N.H. El-Farra, P.D. Christofides, Predictive control of switched nonlinear systems with scheduled mode transitions, IEEE Trans. Autom. Control 50 (11) (Nov. 2005) 1670–1680, https://doi.org/10.1109/TAC.2005.858692.

[23] P. Mhaskar, Robust model predictive control design for fault-tolerant control of process systems, Ind. Eng. Chem. Res. 45 (25) (Dec. 2006) 8565–8574, https://doi.org/10.1021/ie060237p.

[24] R. Liu, Y. Li, 2022, A review of fault tolerant control based on Model Predictive Control, in 2022 37th Youth Academic Annual Conference of Chinese Association of Automation (YAC), Nov., pp. 818–823. doi: 10.1109/YAC57282.2022.10023667.

[25] N.H. El-Farra, P.D. Christofides, Coordinating feedback and switching for control of hybrid nonlinear processes, AIChE J. 49 (8) (2003) 2079–2098, https://doi.org/10.1002/aic.690490817.

[26] N.H. El-Farra, P. Mhaskar, P.D. Christofides, Output feedback control of switched nonlinear systems using multiple Lyapunov functions, Syst. Control Lett. 54 (12) (Dec. 2005) 1163–1182, https://doi.org/10.1016/j.sysconle.2005.04.005.

[27] P. Mhaskar, A. Gani, N.H. El-Farra, C. McFall, P.D. Christofides, J.F. Davis, Integrated fault-detection and fault-tolerant control of process systems, AIChE J. 52 (6) (2006) 2129–2148, doi: 10.1002/aic.10806.

[28] P. Mhaskar, A. Gani, P.D. Christofides, Fault-tolerant control of nonlinear processes: performance-based reconfiguration and robustness, Int. J. Robust. Nonlinear Control 16 (3) (2006) 91–111, doi: 10.1002/rnc.1045.

[29] P. Mhaskar, C. McFall, A. Gani, P.D. Christofides, J.F. Davis, Fault-tolerant control of nonlinear systems: fault-detection and isolation and controller reconfiguration, *2006 Am. Control Conf.* (Jun. 2006) 8, pp.-. doi: 10.1109/ACC.2006.1657534.

[30] P. Mhaskar, A. Gani, C. McFall, P.D. Christofides, J.F. Davis, Fault-tolerant control of nonlinear process systems subject to sensor faults, AIChE J. 53 (3) (2007) 654–668, doi: 10.1002/aic.11100.

[31] R. Gandhi, P. Mhaskar, Safe-parking of nonlinear process systems, Comput. Chem. Eng. 32 (9) (Sep. 2008) 2113–2122, https://doi.org/10.1016/j.compchemeng.2008.03.002.

[32] M. Mahmood, R. Gandhi, P. Mhaskar, Safe-parking of nonlinear process systems: handling uncertainty and unavailability of measurements, Chem. Eng. Sci. 63 (22) (Nov. 2008) 5434–5446, https://doi.org/10.1016/j.ces.2008.07.033.

[33] M. Du, P.M haskar, Uniting safe-parking and reconfiguration-based approaches for fault-tolerant control of switched nonlinear systemsProc. 2010 Am. Control Conf. Jun. 20102829283410.1109/ACC.2010.5531434.

[34] M. Du, P. Mhaskar, A safe-parking and safe-switching framework for fault-tolerant control of switched nonlinear systems,", Int. J. Control 84 (1) (Jan. 2011) 9–23, https://doi.org/10.1080/00207179.2010.536852.

[35] R. Ranjan, L. Das, N.S. Kaisare, R. Srinivasan, A testbed for studying the interactions between human operators and advanced control systems, Comput. Chem. Eng. 178 (Oct. 2023) 108377, https://doi.org/10.1016/j.compchemeng.2023.108377.

[36] E.Badreddin, M.Abdel-Geliel, Dynamic safety margin principle and application in control of safety critical systemsProc. 2004 IEEE Int. Conf. Control Appl., 2004.1Sep. 200468969410.1109/CCA.2004.1387293.

[37] M.Abd-Elgeliel, E.Badreddin, Adaptive controller using dynamic safety margin for hybrid laboratory plantProc. 2005, Am. Control Conf., 2005.2Jun. 20051443144810.1109/ACC.2005.1470168.

[38] M.Abdel-Geliel, E.Badredden, A.Gambier, Application of Dynamic Safety Margin in robust fault detection and fault tolerant control,"2006 IEEE Conf. Comput. Aided Control Syst. Des., 2006 IEEE Int. Conf. Control Appl., 2006 IEEE Int. Symp. . Intell. ControlOct. 200633734210.1109/CACSD-CCA-ISIC.2006.4776669.

[39] M.Abdel-Geliel, E.Badreddin A.Gambier, Application of model predictive control for fault tolerant system using dynamic safety margin2006 Am. Control Conf.Jun. 20066 pp.10.1109/ACC.2006.1657598.

[40] M.Abdel-Geliel, "Controller design and adaptation based on Dynamic Safety Margin,"2008 12th Int. Middle-East Power Syst. Conf. Mar. 200817217710.1109/MEPCON.2008.4562338.

[41] J. Ariamuthu Venkidasalapathy, C. Kravaris, Safety-centered process control design based on dynamic safe set, J. Loss Prev. Process Ind. 65 (May 2020) 104126, https://doi.org/10.1016/j.jlp.2020.104126.

[42] P. Du, J.A. Venkidasalapathy, S. Venkateswaran, B. Wilhite, C. Kravaris, Model-based fault diagnosis and fault tolerant control for safety-critical chemical reactors: a case study of an exothermic continuous stirred-tank reactor, Ind. Eng. Chem. Res. 62 (34) (Aug. 2023) 13554–13571, https://doi.org/10.1021/acs.iecr.3c01205.

[43] L.E. Olivier, I.K. Craig, "Should I shut down my processing plant? An analysis in the presence of faults," Journal of Process Control, Volume 56, 2017, Pages 35-47, ISSN 0959-1524, https://doi.org/10.1016/j.jprocont.2017.05.005.

[44] S. Venkateswaran, C. Kravaris, Disturbance decoupled functional observers for fault estimation in nonlinear systems, Am. Control Conf. (ACC), Tor., Can. (July 2024) 1518–1524, https://doi.org/10.23919/ACC60939.2024.10644495.

[45] K. Hirata, Y. Ohta, Exact determinations of the maximal output admissible set for a class of nonlinear systems, Automatica 44 (2) (Feb. 2008) 526–533, https://doi.org/10.1016/j.automatica.2007.06.016.

[46] M. Rachik, A. Tridane, M. Lhous, O.I. Kacemi, Z. Tridane, Maximal output admissible set and admissible perturbations set for nonlinear discrete systems, Appl. Math. Sci. 1 (32) (2007) 1581–1598.

[47] I.Kolmanovsky, E.G.Gilbert, Maximal output admissible sets for discrete-time systems with disturbance inputsProc. 1995 Am. Control Conf. - ACC'95, Seattle, WA, USA: Am. Autom. Control Counc.19951995199910.1109/ACC.1995.531239.

[48] E.G. Gilbert, K.T. Tan, Linear systems with state and control constraints: the theory and application of maximal output admissible sets, IEEE Trans. Autom. Control 36 (9) (Sep. 1991) 1008–1020, doi: 10.1109/9.83532.

[49] K.Hirata, Y.Ohta, The maximal output admissible set for a class of uncertain systems," in , Dec. 2004, pp. 2686-2691vol.3. doi: 10.1109/CDC.2004.1428866.2004 43rd IEEE Conference on Decision and Control (CDC) (IEEE Cat. No.04CH37601).

[50] H.S. Fogler, *Elements of chemical reaction engineering*, 5th ed, Prentice Hall, 2016.