Incipient Actuator Fault Handling in Nonlinear Model Predictive Control

Brage Rugstad Knudsen [*] **Timm Faulwasser** [**,***]
Colin N. Jones [***] **Bjarne Foss** [*]

[*] *Department of Engineering Cybernetics, Norwegian University of Science and Technology, N-7491 Trondheim, Norway (e-mail: {brage.knudsen, bjarne.foss}@ntnu.no).*
[**] *Institute for Applied Computer Science, Karlsruhe Institute of Technology, 76131 Karlsruhe, Germany, (e-mail: timm.faulwasser@kit.edu).*
[***] *Laboratoire d'Automatique, École Polytechnique Fédérale de Lausanne (EPFL), Lausanne, Switzerland (e-mail: colin.jones@epfl.ch).*

Abstract: This paper presents a reconfigurable nonlinear model predictive control (NMPC) scheme for handling of incipient actuator faults in nonlinear plants. The scheme seeks to ensure recoverability from an incipient actuator fault in plants where the input redundancy is insufficient to stabilize the faulty system at the nominal operating point, thereby requiring transition to a safe control-invariant set. To this end, the proposed scheme takes into account an estimate of the decrease in remaining actuator capacity from the time of detection of an incipient actuator fault, and minimizes the required control input to steer the plant to the safe set. We provide conditions for stability and fault recoverability of the proposed scheme, and demonstrate its applicability on a numerical example with two CSTRs in series.

Keywords: Nonlinear Model Predictive Control, Fault-tolerant Control, Process Control

1. INTRODUCTION

Model predictive control (MPC) has emerged as an attractive control scheme for embedding fault tolerance, from its ability to both optimize performance of complex constrained systems while accommodating system faults through online adaptation of the internal MPC model (Maciejowski, 1999). While several robust, passive fault-tolerant MPC (FTMPC) approaches have been developed, e.g. Maciejowski (1999), the majority of FTMPC schemes belong to the class of active (reconfigurable) fault-tolerant control (FTC) schemes. A variety of active FTMPC schemes have been developed to handle actuator and system faults, e.g. Yetendje et al. (2013); Franzè et al. (2015); Knudsen (2016), and sensor faults (Yetendje et al., 2010; Xu et al., 2014; Knudsen et al., 2016).

While fault accommodation through online reconfiguration makes MPC attractive for FTC, there are many systems with structures or control policies that impede such simple reactive fault accommodation: An NMPC controller may require availability of a sufficient control input in order to robustly operate a plant in a small region about the nominal steady state. If an actuator fails or the input capacity decreases, then a small disturbance may cause a finite time escape of some of the plant's states. An example of the latter is process systems with exothermic reactions, where it is often desirable to operate the plant at an unstable steady state to achieve sufficient conversion rates while avoiding high temperatures (El-Farra et al., 2005). Moreover, economic operation of a plant, e.g. through economic MPC, tends to drive the system close to the boundary of the feasible region (Lucia et al., 2014), in which an actuator fault may reduce the MPC feasible region and hence cause constraint violations.

Guaranteeing recoverability from an actuator fault for an NMPC controlled plant may require a high degree of control-input redundancy, or operation of the plant a conservative state that warrants recovery from any fault scenario. As an alternative, several preventive or proactive FTMPC schemes have been proposed (Lao et al., 2013; Bø and Johansen, 2014; Knudsen, 2016; Albalawi et al., 2016). Proactive FTMPC schemes seek to enable a plant to operate in nominal mode, relying on a fault detection and isolation (FDI) unit to be designed so as to detect sufficiently early the onset of an incipient fault, upon which the FTMPC controller proactively steers the plant to a safe set or steady state. These schemes, however, as well as the related reactive safe-parking schemes, e.g. Amui and Mhaskar (2009), all assume sufficient remaining controllability of the healthy actuators to steer the plant to the safe set or steady state. Yet, such safe transition of the operating point of a plant may require using the faulty actuator, in which the controller must take into account the gradual decrease in remaining available input capacity.

In this paper, we propose a fault-tolerant NMPC (FTNMPC) scheme that takes into account a gradual decreasing input-capacity resulting from an incipient actuator fault. The main contribution is the design of a reconfigurable, stabilizing NMPC scheme for plants that require using the faulty actuator in order to steer the plant from a nominal setpoint to a safe park. The remainder of the paper is structured as follows: In Section 2 we present the system and problem structure. Section 3 describes the design of the proposed FTNMPC scheme, with stability properties described in Section 4. In Section 5, we illustrate the proposed scheme through simulations of a two-series CSTR. Section 6 ends the paper with concluding remarks.

2. PROBLEM STATEMENT

2.1 System Description

In this paper, we consider nonlinear discrete-time systems

$$x_{k+1} = f(x_k, u_k), \tag{1}$$

where $x_k \in \mathbb{R}^{n_x}$ is the state of the system, $u_k \in \mathbb{R}^{n_u}$ with $n_u > 1$, the input, and where $f : \mathbb{R}^{n_x} \times \mathbb{R}^{n_u} \mapsto \mathbb{R}^{n_x}$ is twice continuously differentiable. We denote the set $\mathcal{I} := \{1, \ldots, n_u\}$ as the set of inputs for (1). The control of the plant described by (1) is subject to state constraints,

$$x_k \in \mathbb{X} \subseteq \mathbb{R}^n, \tag{2}$$

and input box constraints of the form

$$-\bar{u} \leq u_k \leq \bar{u}, \tag{3}$$

where $\bar{u} \in \mathbb{R}^m$ is a vector of capacity constraints on the inputs. The set $\mathbb{X}$ is assumed compact and time invariant. We denote $x(t)$ as the state of the system at time t, and we assume that the full state can be measured. Furthermore, we use $k \in \mathbb{Z}_{[a,b]}$ to denote the discrete time-index for the predictions, where $\mathbb{Z}$ is the set of integers on the interval $[a, b]$. During nominally conditions, we assume that the system (1) is stabilized at a feasible steady state $(x_{\mathrm{s}}, u_{\mathrm{s}})$ by a nominal NMPC controller, see e.g. Mayne et al. (2000). Consequently, we focus in the sequel on the formulation and design of the FTNMPC scheme.

2.2 Problem Description

We consider the problem of stabilizing the plant described by (1) subject to an incipient fault in actuator u_j $j \in \mathcal{I}$. Incipient faults, in contrast to abrupt step-wise faults, are characterized by slowly developing performance degradation of the faulty component. This performance degradation can be described by a time profile (or decrease function) (Zhang et al., 2002) which we will denote as $\psi(t, t^{\mathrm{fa}}) \in [0, 1]$. As we focus on the design of an NMPC controller that properly accommodates an incipient actuator fault, we make the following fault-detectability assumption:

Assumption 1. At time t^{fa} (fault alarm), an FDI unit detects the onset of an incipient fault in actuator $u_j, j \in \mathcal{I}$, and provides a *worst-case* estimate $\hat{\psi}(t, t^{\mathrm{fa}}) \leq \psi(t, t^{\mathrm{fa}})$, with $\hat{\psi} : t \mapsto \mathbb{R}$ monotonically decreasing, of the decrease in remaining capacity of the faulty actuator. The incipient fault occurs in one control input only.

For incorporation in a discrete-time NMPC formulation, we denote $\hat{\psi}_{t+k}$ as the discrete-time values of the estimate $\hat{\psi}(t, t^{\mathrm{fa}})$ predicted k timesteps ahead from time t. The time profile of incipient faults, and hence the decrease in remaining actuator capacity, is often modeled as exponential relations, see e.g. Zhang et al. (2002); Demetriou and Polycarpou (1998). Other models may also be considered, including linear and Sigmoidal profiles, as well as probabilistic approaches (Salfner, 2007).

The decreasing capacity of actuator j naturally affects the input box constraints (3). Let $\Theta_k \in \mathbb{R}^{m \times m}$ be a time-dependent matrix defined as

$$\Theta_k = \mathrm{diag}\left(\left[1, \ldots, 1, \hat{\psi}_{t+k}, 1, \ldots, 1\right]\right), \tag{4}$$

i.e. with element Θ_{kjj} equal to $\hat{\psi}_{t+k}$. The reduced input capacity of actuator j can then be simply incorporated by modifying (3) as

$$-\Theta_k \bar{u} \leq u_k \leq \Theta_k \bar{u}. \tag{5}$$

Remark 1. Note that instead of (5), we may define

$$u_k := \Theta_k \tilde{u}_k, \tag{6}$$

and equivalently characterize the reduced input capacity by modifying the plant model and input box constraints as

$$x_{k+1} = f(x_k, \Theta_k \tilde{u}_k), \tag{7}$$

$$-\bar{u} \leq \tilde{u}_k \leq \bar{u}. \tag{8}$$

This latter form is particularly useful for detection of incipient faults, as it enables the use of parameter estimation techniques or dedicated observer schemes for fault diagnosis. For methods on diagnosis of incipient actuator faults, see e.g. Demetriou and Polycarpou (1998); Zhang et al. (2002); Armaou and Demetriou (2008). We further note that one way of obtaining an estimate $\hat{\psi}(t, t^{\mathrm{fa}})$ is through parameter estimation on past input data in a time window prior to the time of fault alarm t^{fa}.

As discussed in Section 1, conventional reactive FTNMPC schemes may fail in recovering a plant from an actuator fault if the faulty system looses stabilizability at the current operating point. This motivates the following problem definition:

Problem 1. Upon detection of an incipient fault in actuator j, stabilize the system (1) at a given safe steady state $x_{\mathrm{s}}^{\mathrm{safe}} \in \mathbb{X}_{\mathrm{f}}^{\mathrm{safe}}$, where $\mathbb{X}_{\mathrm{f}}^{\mathrm{safe}}$ is a safety set for (1), taking explicitly into account the remaining capacity of the faulty actuator.

3. PROPOSED FTNMPC SCHEME

In order to accommodate the incipient fault in actuator j, we resort to a switching of operation mode from a nominal to a safe-transition NMPC controller. The appropriate control action for steering the system from x_{s} to the safety set $\mathbb{X}_{\mathrm{f}}^{\mathrm{safe}}$ lends itself to a trade-off between the control effort and transition time. Using a large control input decreases the transition time to $\mathbb{X}_{\mathrm{f}}^{\mathrm{safe}}$, which in the extreme case resorts to minimum-time control. On the other hand, using the control input aggressively may cause additional damage to the faulty actuator, thereby advancing the complete failure of the actuator. Minimizing the control input of the faulty actuator in a safe-transition to a safety set thus alleviates the danger of sudden actuator breakdown. Consequently, the NMPC safe-transition mode should enable optimization of the desired control action as a function of the characteristics of the incipient fault such as the observed decrease of actuator capacity at the time of detection and operation time of the faulty component.

While safety sets for (1) may be formulated based on known properties of the plant or through the maximum controlled invariant set with the faulty actuator inactive, such safety sets may be computationally intractable for nonlinear models or difficult to prove invariant. To formulate a generic safety set, we thus propose to impose the safety set $\mathbb{X}_\mathrm{f}^\mathrm{safe}$ through computation of an NMPC terminal constraint set. To this end, we first *precompute* a shifted steady-state $x_\mathrm{s}^\mathrm{safe}$ by solving the steady-state problem

$$\begin{aligned}(x_\mathrm{s}^\mathrm{safe}, u_\mathrm{s}^\mathrm{safe}) = \arg\min\{g(x,u) \mid x = f(x,u), x \in \mathbb{X},\\ -\bar{u}_i \le u_i \le \bar{u}_i, \forall i \in \mathcal{I} \setminus j, u_j = 0\},\end{aligned} \quad (9)$$

where $g(x,u)$ is some, typically economic, performance measure of the plant set by a supervisory level, seeking to preserve a minimum level of economic performance when operating the plant inside the safety set of the faulty actuator. We assume that the plant described by (1)–(3) admits a steady state pair $(x_\mathrm{s}^\mathrm{safe}, u_\mathrm{s}^\mathrm{safe})$ with $u_j = 0$, and that $x_\mathrm{s}^\mathrm{safe}$ is in the interior of $\mathbb{X}$ with $-\bar{u} < u_\mathrm{s}^\mathrm{safe} < \bar{u}$. Observe that we must compute the solution to (9) for each set of actuator fault-scenarios, however, by an offline procedure. Note also that by Assumption 1, we restrict our study to single actuator faults.

To steer the plant into the safety set $\mathbb{X}_\mathrm{f}^\mathrm{safe}$ by means of the provided estimate of remaining input capacity, we update the setpoints and switch from the nominal NMPC controller to solving the safe-transition problem $P^\mathrm{safe}(x,t)$:

$$\begin{aligned}V_N^\mathrm{safe}(x,t) = \min_{x,u,\xi,\gamma} \sum_{k=0}^{N-1} l(x_k - x_\mathrm{s}^\mathrm{safe}, u - u_\mathrm{s}^\mathrm{safe})\\ + \frac{1}{2}\left(\rho_\gamma \gamma^2 + \rho_\xi \xi_0^2\right) + V_\mathrm{f}^\mathrm{safe}(x_N - x_\mathrm{s}^\mathrm{safe})\end{aligned} \quad (10a)$$

$$\begin{aligned}
\text{s.t. } & x_{k+1} = f(x_k, u_k), && k \in \mathbb{Z}_{[0,N-1]}, && (10b)\\
& x_0 = x(t), && && (10c)\\
& x_k \in \mathbb{X}, && k \in \mathbb{Z}_{[0,N-1]}, && (10d)\\
& -\bar{u}_i \le u_{ik} \le \bar{u}_i,\ \forall i \in \mathcal{I} \setminus j, && k \in \mathbb{Z}_{[0,N-1]}, && (10e)\\
& |u_{jk}| \le \bar{u}_j \xi_k \hat{\psi}_{t+k}, && k \in \mathbb{Z}_{[0,N-1]}, && (10f)\\
& \xi_{k+1} \le \gamma \xi_k, && k \in \mathbb{Z}_{[0,N-1]}, && (10g)\\
& 0 \le \xi_k \le 1, && k \in \mathbb{Z}_{[0,N]} && (10h)\\
& 0 \le \gamma \le 1, && && (10i)\\
& x_N \in \mathbb{X}_\mathrm{f}^\mathrm{safe}. && && (10j)
\end{aligned}$$

In (10), $l(x,u) := \frac{1}{2}\left|\left|x\right|\right|_Q^2 + \frac{1}{2}\left|\left|x\right|\right|_R^2$ is a quadratic stage cost with positive definite matrices Q and R, $\xi_k \in \mathbb{R}$ are auxiliary variables for penalizing the input usage, required through (10g) to be exponentially decreasing, while the nonnegative variable $\gamma \in \mathbb{R}$ controls the decrease rate in use of u_j. By including the term $1/2(\rho_\gamma \gamma^2 + \rho_\xi \xi_0^2)$ in (10a), where $\rho_\gamma \ge 0$ and $\rho_\xi \ge 0$ are tuning parameters, we enable tuning with respect to the trade-off between short transition time or low input usage. In particular, $P^\mathrm{safe}(x,t)$ enables a safe-transition control policy that assures the plant to be steered to a safe set $\mathbb{X}_\mathrm{f}^\mathrm{safe}$ within the prediction horizon, while at the same time optimizing on the exponential decay constant γ and the margin ξ_0 to the current remaining capacity of the faulty actuator. The values of ρ_γ and ρ_ξ would normally be set by a supervisory level as a function the severity and time of detection of the incipient fault. Observe that by Assumption 1, $\hat{\psi}_{t+k}$ is a worst-case decrease of the remaining capacity of actuator j, and that this estimate is kept constant and only shifted forward in time in $P^\mathrm{safe}(x,t)$.

3.1 Terminal Safety Set

In order for $P^\mathrm{safe}(x,t)$ to stabilize the faulty system at the safe steady state $x_\mathrm{s}^\mathrm{safe}$, we must construct an appropriate terminal set $\mathbb{X}_\mathrm{f}^\mathrm{safe}$ and terminal cost $V_\mathrm{f}^\mathrm{safe}(\cdot)$. To ease this design, we make a change of coordinates,

$$z = x - x_\mathrm{s}^\mathrm{safe}, \quad (11a)$$

$$v = u - u_\mathrm{s}^\mathrm{safe}, \quad (11b)$$

from which we redefine the plant dynamics (1) as

$$\begin{aligned}z_{k+1} &= f\left(z_k + x_\mathrm{s}^\mathrm{safe}, v_k + u_\mathrm{s}^\mathrm{safe}\right) - x_\mathrm{s}^\mathrm{safe},\\ &:= \bar{f}(z_k, v_k),\end{aligned} \quad (12)$$

such that $\bar{f}(0,0) = 0$. The state and input constraints are updated accordingly, where we denote $\bar{\mathbb{X}}$ and $\bar{v}$ as the shifted state and input box-constraints, respectively. Moreover, for notational convenience, we define a modified stage cost

$$\bar{l}\left(z, v, \gamma, \xi_0\right) := l(z,v) + \frac{\rho}{N-1}(\gamma^2 + \xi_0^2), \quad (13)$$

with $\bar{l}(0,0,0,0) = 0$. For the design of the terminal set, we invoke the following stabilizability assumption:

Assumption 2. The pair (A, B_j^f) of the linearized system $z_{k+1} = Az_k + B_j^\mathrm{f} v_k$ is stabilizable, where $A = \frac{\partial \bar{f}}{\partial z}(0,0)$ and $B_j^\mathrm{f} = B \cdot \mathrm{diag}([1,1,\ldots,\beta_j,1,\ldots,1])$, with $\beta_j = 0$ and $B = \frac{\partial \bar{f}}{\partial v}(0,0)$. Furthermore, $\bar{f}(\cdot,\cdot)$ is twice continuously differentiable.

This latter assumption enables construction of a linear state-feedback controller $v_k = K_j z_k$ that exponentially stabilizes the linearized system $z_{k+1} = (A + B_j^\mathrm{f} K_j) z_k$. Observe that K_j sets the faulty input to 0. By ensuring that the terminal cost $V_\mathrm{f}^\mathrm{safe}(\cdot)$ satisfies

$$\begin{aligned}V_\mathrm{f}^\mathrm{safe}(\bar{f}(z, K_j z), t) - V_\mathrm{f}^\mathrm{safe}(z,t) \le -\bar{l}(z, K_j z, 0, 0),\\ \forall z \in \bar{\mathbb{X}}_\mathrm{f}^\mathrm{safe},\end{aligned} \quad (14)$$

and choosing $\bar{\mathbb{X}}_\mathrm{f}^\mathrm{safe} \subset \bar{\mathbb{X}}$ with $0 \in \bar{\mathbb{X}}_\mathrm{f}^\mathrm{safe}$ as a suitable ellipsoidal level set of $V_\mathrm{f}^\mathrm{safe}(\cdot)$,

$$\bar{\mathbb{X}}_\mathrm{f}^\mathrm{safe} := \left\{ z \in \mathbb{R}^n \;\middle|\; \frac{1}{2} z' P z \le \alpha \right\}, \quad (15)$$

where α is a positive constant and P a positive definite matrix, we can assure that the linear state feedback $v_k = K_j z_k$ stabilizes the origin of the closed-loop system $z_{k+1} = \bar{f}(z_k, K_j z_k)$ inside $\bar{\mathbb{X}}_\mathrm{f}^\mathrm{safe}$. By designing $\bar{\mathbb{X}}_\mathrm{f}^\mathrm{safe}$ as a level set of $V_\mathrm{f}^\mathrm{safe}(\cdot)$, we further assure that $\bar{\mathbb{X}}_\mathrm{f}^\mathrm{safe}$ is positively invariant under the control law $v_k = K_j z_k$ (Mayne et al., 2000). To design the terminal set $\bar{\mathbb{X}}_\mathrm{f}^\mathrm{safe}$ and cost $V_f^\mathrm{safe}(\cdot)$ that satisfies (14) and (15), we adopt a discrete-time variant of Chen and Allgöwer (1998) as outlined in Johansen (2004), with an iterative procedure for computing a value of α that satisfies (14).

It is worth pointing out that while we do not necessarily have sufficient actuator redundancy to stabilize the faulty system at the nominal equilibrium point, we require the system to be stabilizable by the $n_u - 1$ healthy actuators at the safe steady state.

4. PROPERTIES OF PROPOSED FTNMPC SCHEME

In this section, we establish conditions for stability and recursive feasibility of $P^{\text{safe}}(x,t)$, using the translated system (12). To this end, we denote $z_s = x_{\text{s}} - x_{\text{s}}^{\text{safe}}$ as the nominal steady state in the translated system.

For the safe-transition problem $P^{\text{safe}}(x,t)$, the following *nominal* stability property holds:

Theorem 3. (Stability of safe steady state).
If

(i) Assumption 1 and 2 hold.
(ii) $P^{\text{safe}}(x,t)$ is feasible at time t^{fa}.

Then $P^{\text{safe}}(x,t)$ is recursively feasible, and $(x_{\text{s}}^{\text{safe}}, u_{\text{s}}^{\text{safe}})$ is a locally asymptotic stable steady state of the closed-loop system under the safe-transition NMPC control law.

Proof. Feasibility of $P^{\text{safe}}(x,t)$ at time t^{fa} implies reachability of $\bar{\mathbb{X}}_{\text{f}}^{\text{safe}}$ from z_{s}. Within $\bar{\mathbb{X}}_{\text{f}}^{\text{safe}}$, the linear feedback $v = K_j z$ with $\xi_k = 0$ is admissible for problem $P^{\text{safe}}(x)$. By Assumption 1, then at time $t^{\text{fa}}+1$, the optimal input sequence $\{v_0, v_1, \dots, v_{N-1}\}$, shifted one step ahead and appended with $K_j z_N$ satisfies the shifted time-varying input constraints $|v_{jk}| \leq \xi_k \bar{v}_j \hat{\psi}_{t+1+k}$, since K_j is designed with $v_j = u_j = 0$, ensuring that $K_j z_N$ is feasible with $\xi_N = 0$. Similarly, the sequence $\{\xi_0, \xi, \dots, \xi_{N-1}, \xi_N\}$ computed at time t^{fa} shifted one step ahead and appended with 0 is feasible for $P^{\text{safe}}(x)$ at time $t^{\text{fa}}+1$. The monotonicity assumption of $\hat{\psi}$ with the required exponential decrease of ξ_k assures that the optimal decay rate γ computed at time t^{fa} is also feasible at time $t^{\text{fa}}+1$. Hence, using standard arguments, the construction of the positively invariant terminal region $\bar{\mathbb{X}}_{f}^{\text{safe}}$ implies recursive feasibility of $P^{\text{safe}}(x,t)$, cf. Chen and Allgöwer (1998, Lm. 2).

For stability, we first note that $V_{\text{f}}^{\text{safe}}(\cdot)$ and $\bar{\mathbb{X}}_{\text{f}}^{\text{safe}}$ are by design time invariant, $\bar{\mathbb{X}}_{\text{f}}^{\text{safe}}$ contains the origin in its interior, and $\bar{l}(\cdot)$ is convex with $\bar{l}(0,0,0,0) = 0$. Furthermore, the additional variables γ and ξ_0 in the stage cost are both bounded, and can be considered as additional input variables to v. Inside $\bar{\mathbb{X}}_{\text{f}}^{\text{safe}}$, $\gamma = 0$ and $\xi_k = 0, \forall k \in \mathbb{Z}_{[0,N]}$ is feasible. By Assumption 2, $V_{\text{f}}^{\text{safe}}(\cdot)$ can be bounded above by a class $\mathcal{K}$ function in $\bar{\mathbb{X}}_{\text{f}}^{\text{safe}}$. Moreover, if $P^{\text{safe}}(x)$ is feasible at time t^{fa}, the cost of steering the system from z_{s} to $\bar{\mathbb{X}}_{\text{f}}^{\text{safe}}$ is bounded. We can thus apply Prop. 2.35 of Rawlings and Mayne (2009) to establish time independent lower and upper bounds on the optimal cost $V_N^{\text{safe}}(x,t)$ by class $\mathcal{K}$ functions. This ensures that $V_N^{\text{safe}}(x,t)$ satisfies a value function also in the time-varying case, as well as by design of the terminal cost and constraints, satisfies a Lyapunov-like cost decrease. Hence, we can by Th. 2.37, p.131 in Rawlings and Mayne (2009), conclude asymptotic stability of the origin for the translated closed-loop system under the NMPC control law, and hence for $(x_{\text{s}}^{\text{safe}}, u_{\text{s}}^{\text{safe}})$ by (11). □

Observe that solving (9) does not necessarily render a steady state with a stabilizable linearization as defined in Assumption 2. This must be checked a posteriori and, if necessary, with tightening of the state and input constraints in (9) in order to achieve a stabilizable linearization around $(x_{\text{s}}^{\text{safe}}, u_{\text{s}}^{\text{safe}})$. Furthermore, one may encounter situations where $(x_{\text{s}}^{\text{safe}}, u_{\text{s}}^{\text{safe}})$ and $(x_{\text{s}}, u_{\text{s}})$ coincide, that is, the nominal steady state is actually optimal and safe stabilizable with $u_j = 0$.

The following proposition follows from Theorem 3.

Proposition 4. (Fault recoverability). The NMPC problem $P^{\text{safe}}(x,t)$ solved on a receding horizon with $\bar{\mathbb{X}}_{\text{f}}^{\text{safe}}$ and $V_{\text{f}}^{\text{safe}}(\cdot)$ described in Section 3.1 solves Problem 1.

Remark 5. Infeasibility of $P^{\text{safe}}(x,t)$ at time t^{fa} implies a failure of the proposed FTNMPC scheme in stabilizing the faulty system. That is, the fault-tolerant controller fails in preventing a fault from developing into an actuator failure. In this case, some emergency mode must be activated.

Remark 6. For abrupt-like faults, $\psi(t, t^{\text{fa}})$ approaches or is equal to the unit step function. The proposed framework also covers this scenario, leaving $\xi_k = 0$ and $\gamma = 0$, with conditions for stability and fault recoverabilty equal to Theorem 3. However, while we consider fault recovery that explicitly requires use of the faulty actuator, fault recoverability by $P^{\text{safe}}(x,t)$ from abrupt fault depends on whether the plant actually can be stabilized at $x_{\text{s}}^{\text{safe}}$ by means of the healthy inputs only.

5. NUMERICAL EXAMPLE

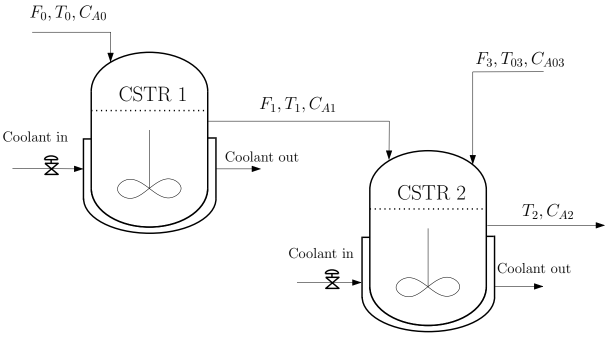

Fig. 1. Illustration of two CSTRs in series.

To illustrate the proposed FTNMPC controller, we consider an example with two non-isothermal continuous stirred-tank reactors (CSTRs) in series, adopted from El-Farra et al. (2005). The interconnections of the two CSTRs are illustrated in Fig. 1. In each CSTR, three parallel irreversible elementary exothermic reactions of the form $A \xrightarrow{k_1} B$, $A \xrightarrow{k_2} U$ and $A \xrightarrow{k_3} R$ take place, where A is the reactant and B is the desired product. U and R are undesired byproducts. Individual jackets are used to remove heat from or supply heat to each reactor. We assume that the temperature and composition of the CSTRs are uniform. The feed to CSTR 1 consists of pure A at a flow rate F_0, molar concentration C_{A0}, and temperature T_0, while the feed to CSTR 2 consists of the output from CSTR 1, together with an additional fresh stream feeding pure A at flow rate F_3, molar concentration C_{A03}, and temperature T_{03}. The resulting interconnected CSTR model reads

$$\begin{aligned}\frac{dT_1}{dt} &= \frac{F_0}{V_1}(T_0 - T_1) \\ &\quad + \sum_{i=1}^{3} \frac{(-\Delta H_i)}{\rho c_{\text{p}}} r_i(C_{A1}, T_1) + \frac{Q_1}{\rho c_{\text{p}} V_1},\end{aligned} \tag{16a}$$

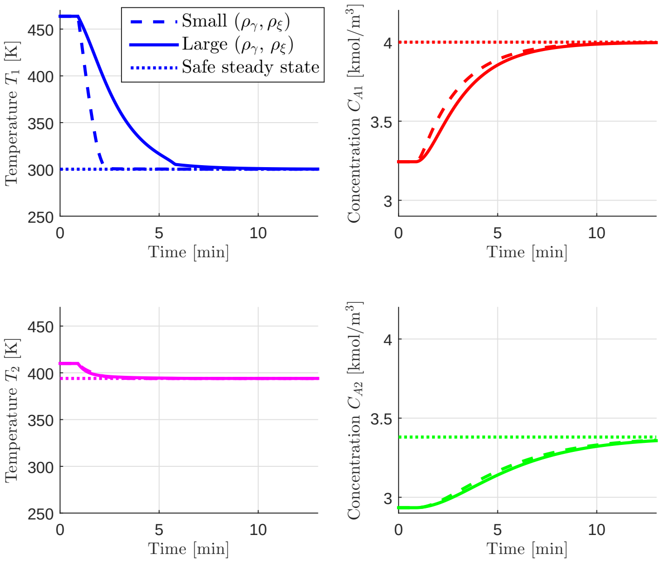

Fig. 2. Closed loop states of the proposed FTNMPC scheme applied to (16) with small (dashed lines) and large (solid lines) values for ρ_γ and ρ_ξ, respectively.

$$\frac{dC_{A1}}{dt} = \frac{F_0}{V_1}(C_{A0} - C_{A1}) - \sum_{i=1}^{3} r_i(C_{A1}, T_1), \tag{16b}$$

$$\begin{aligned} \frac{dT_2}{dt} &= \frac{F_1}{V_2}(T_1 - T_2) + \frac{F_3}{V_2}(T_{03} - T_2) \\ &\quad + \sum_{i=1}^{3} \frac{(-\Delta H_i)}{\rho c_{\mathrm{p}}} r_i(C_{A2}, T_2) + \frac{Q_2}{\rho c_{\mathrm{p}} V_2}, \end{aligned} \tag{16c}$$

$$\begin{aligned} \frac{dC_{A2}}{dt} &= \frac{F_1}{V_2}(C_{A1} - C_{A2}) + \frac{F_3}{V_2}(C_{A03} - C_{A2}) \\ &\quad - \sum_{i=1}^{3} r_i(C_{A2}, T_2), \end{aligned} \tag{16d}$$

where

$$r_i(C_{Ad}, T_d) = k_{i0} e^{-\frac{E_i}{RT_d}} C_{Ad}, \qquad d = 1, 2 \tag{17}$$

are the reaction rates. The inputs of (16) are the jacket heat rates, $u_i = Q_i$ for $i = 1, 2$, with available control energy $|Q_1| \leq \bar{Q}_1 = 2.7 \times 10^3$ kJ/h and $|Q_2| \leq \bar{Q}_2 = 2.8 \times 10^3$ kJ/h. For numerical values of the parameters in(16), we refer the reader to El-Farra et al. (2005).

The CSTR model (16) is discretized in time using the backward Euler method. We initialize the system at the nominal steady-state $x_{\mathrm{s}} = (T_{1s}, C_{A1s}, T_{2s}, C_{A2s}) = (463.71, 3.24, 410.00, 2.93)$, which is an unstable steady state for CSTR 1 while stable for CSTR 2, and assume that the control system receives a warning about an incipient fault in actuator $u_1 = Q_1$ at $t^{\mathrm{fa}} = 1$ min. To compute $x_{\mathrm{s}}^{\mathrm{safe}}$ through (9), we set the economic objective $g(x, u) = -\sum_{d=1}^{2} r_1(C_{Ad}, T_d)$, that is, we compute $x_{\mathrm{s}}^{\mathrm{safe}}$ as a steady state where the reaction rates of the desired product B can be safely maximized with $Q_1 = 0$. This approach yields $x_{\mathrm{s},j}^{\mathrm{safe}} = (300.17, 3.99, 394.00, 3.38)$, which is verified to be a stabilizable steady state for (16) with $Q_1 = 0$. We implement the NMPC in GAMS, using IPOPT (Wächter and Biegler, 2005) with a prediction horizon of $N = 150$ (i.e. 9 min) and a sampling time of 3.6s to solve the NLPs.

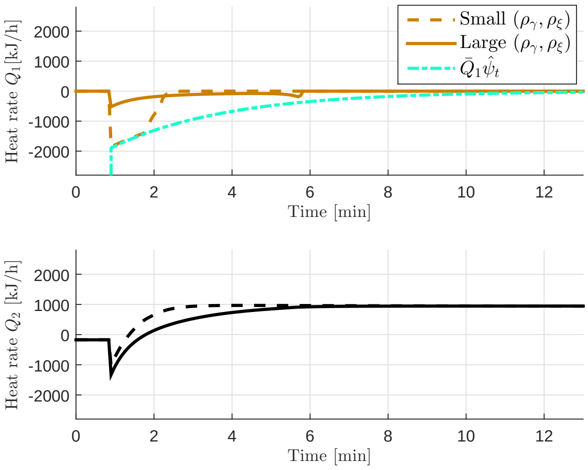

Fig. 3. Control inputs with an incipient fault in the cooling for CSTR 1. The dashed lines shows the simulation with small values for ρ_γ and ρ_ξ, while the solid lines shows simulations with corresponding large values for ρ_γ and ρ_ξ. The time decrease-profile of the faulty actuator is shown with a cyan dashed-dotted line.

In the considered example, incipient actuator faults take may place include a slowly decrease in available cooling/heating capacities due to leakages in the jacket system, and fouling in the jacket control-valves. For the simulations, we consider a scenario where an incipient fault is detected the first reactor when 70% of the heat-rate of capacity Q_1 is remaining. Following Zhang et al. (2002), we further assume that the worst-case estimate of the reaming cooling capacity can be characterized by $\hat{\psi}_t = \mu_1 e^{-\mu_2(t - t^{\mathrm{fa}})}$, with $\mu_1 = 0.7$ and $\mu_2 = 0.02$. For the terminal set and cost described in Section 3.1, we compute K_j as the LQR optimal gain matrix and P from the associated Lyapunov equation for the linearized closed-loop system, see Chen and Allgöwer (1998) and Rawlings and Mayne (2009, Ch. 2.6) for details.

Fig. 2 and 3 show the states and inputs for (16) from simulations of the FTNMPC scheme with two sets of values for ρ_γ and ρ_ξ. Imposing large values for ρ_γ and ρ_ξ is seen to render a cautious use of the faulty control input Q_1 with a large margin ξ_0 to $\bar{Q}_1\hat{\psi}_t$. In comparison, imposing small values to ρ_γ and ρ_ξ causes a more aggressive use of the faulty actuator with an input for a short time-window equal or close to the estimate of the decrease in cooling capacity. This trade-off in utilization of the faulty actuator is clearly reflected in the transition time of T_1 from nominal to safe steady-state, seen in the upper-left plot of Fig. 2. Note that the slow concentration dynamics are less affected by the aggressive and cautious usage of the faulty input, respectively.

For the two CSTRs (16) in series, an abrupt fault in the jacket for CSTR 1 with a conventional *reactive* FTNMPC strategy (see e.g. Yetendje et al. (2013)), where the internal NMPC model is updated first *after* the fault occurs, would destabilize the plant. To illustrate this, we show in Fig. 4 a simulation where the cooling Q_1 is rendered completely useless after time $t = 1$ min. As Q_1 at nominal steady state is 0, cf. Fig 3, the plant remains at x_{s}, while the controller is unable to steer the plant x_s^{safe} since the stabilizability of

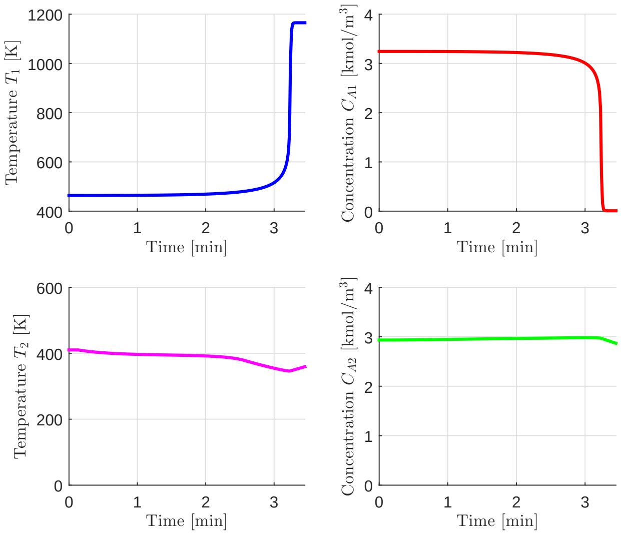

Fig. 4. Simulation of an abrupt fault in the cooling of CSTR 1 with a reactive FTNMPC scheme.

CSTR 1 is lost. For the purpose of illustration, we add a small disturbance to the plant after $t = 4$ min, which is seen to eventually cause a runaway of the temperature T_1. This highlights the necessity for this application to detect an incipient actuator fault sufficiently early, and transfer the plant to a safe steady state.

6. CONCLUDING REMARKS

This paper has presented an FTNMPC scheme for handling of incipient actuator faults in nonlinear plants, where stabilization of the faulty plant requires a safe transition with use of the faulty actuator. The proposed scheme can efficiently complement existing FTC schemes for nonlinear plants. The proposed framework naturally lends itself to an extension with a probabilistic approach for explicitly incorporating uncertainty in the decrease function of the faulty actuator.

7. ACKNOWLEDGMENT

BRK and BF gratefully acknowledges financial support from Cybernetica AS. TF thanks the Baden-Württemberg Stiftung for the financial support of this research by the Elite Programme for Postdocs.

REFERENCES

Albalawi, F., Alanqar, A., Durand, H., and Christofides, P.D. (2016). Simultaneous control of safety constraint sets and process economics using economic model predictive control. In *Proc. Amer. Cont. Conf.*, 5062–5067.

Amui, S. and Mhaskar, P. (2009). Safe-steering of batch process systems. *AIChE J*, 55(11), 2861–2872.

Armaou, A. and Demetriou, M.A. (2008). Robust detection and accommodation of incipient component and actuator faults in nonlinear distributed processes. *AIChE J*, 54(10), 2651–2662.

Bø T.I. and Johansen, T.A. (2014). Dynamic safety constraints by scenario based economic model predictive control. In *Proc. IFAC World Congress*.

Chen, H. and Allgöwer, F. (1998). A quasi-infinite horizon nonlinear model predictive control scheme with guaranteed stability. *Automatica*, 34(10), 1205–1217.

Demetriou, M.A. and Polycarpou, M.P. (1998). Incipient fault diagnosis of dynamical systems using online approximators. *IEEE Trans. Autom. Control*, 43(11), 1612–1617.

El-Farra, N.H., Gani, A., and Christofides, P.D. (2005). Fault-tolerant control of process systems using communication networks. *AIChE J*, 51(6), 1665–1682.

Franzè, G., Tedesco, F., and Famularo, D. (2015). Actuator fault tolerant control: A receding horizon set-theoretic approach. *IEEE Trans. Autom. Control*, 60(8), 2225 – 2230.

Johansen, T.A. (2004). Approximate explicit receding horizon control of constrained nonlinear systems. *Automatica*, 40, 293–300.

Knudsen, B.R. (2016). Proactive actuator fault-tolerance in economic MPC for nonlinear process plants. In *Proc. of IFAC Symp. on Dynamics and Control of Process Systems*. Trondheim, Norway.

Knudsen, B.R., Alessandretti, A., and Jones, C.N. (2016). Sensor fault tolerance in output feedback nonlinear model predictive control. In *Proc. Conf. Control and Fault-Tolerant Sys. (SysTol)*. Barcelona, Spain.

Lao, L., Ellis, M., and Christofides, P.D. (2013). Proactive fault-tolerant model predictive control. *AIChE J*, 59(8), 2810–2820.

Lucia, S., A.E. Andersson, J., Brandt, H., Diehl, M., and Engell, S. (2014). Handling uncertainty in economic nonlinear model predictive control: A comparative case study. *J. Process Control*, 24(8), 1247–1259.

Maciejowski, J.M. (1999). Modelling and predictive control: Enabling technologies for reconfiguration. *Annu. Rev. Control*, 23, 13–23.

Mayne, D.Q., Rawlings, J.B., Rao, C.V., and Scokaert, P.O.M. (2000). Constrained model predictive control : Stability and optimality. *Automatica*, 36(6), 789–814.

Rawlings, J. and Mayne, D. (2009). *Model Predictive Control: Theory and Design*. Nob Hill Publishing.

Salfner, F.and Malek, M. (2007). Using hidden semi-Markov models for effective online failure prediction. In *Proc. IEEE Symp. on Reliable Dist. Syst.*, 161–174.

Wächter, A. and Biegler, L.T. (2005). On the implementation of an interior-point filter line-search algorithm for large-scale nonlinear programming. *Math. Program.*, 106(1), 25–57.

Xu, F., Olaru, S., Puig, V., Ocampo-Martinez, C., and Niculescu, S.I. (2014). Sensor-fault tolerance using robust MPC with set-based state estimation and active fault isolation. In *Proc. Conf. Decision Control*, 4953–4958.

Yetendje, A., Seron, M.M., and De Doná, J.A. (2010). Robust MPC design for fault tolerance of constrained multisensor linear systems. In *Proc. Conf. Control and Fault-Tolerant Sys. (SysTol)*, 4678–4683.

Yetendje, A., Seron, M.M., and Doná, J.A.D. (2013). Robust multiactuator fault-tolerant MPC design for constrained systems. *Int. J. of Robust Nonlin.*, 23(16), 1828–1845.

Zhang, X., Polycarpou, M.M., and Parisini, T. (2002). A robust detection and isolation scheme for abrupt and incipient faults in nonlinear systems. *IEEE Trans. Autom. Control*, 47(4), 576–593.