Proactive Actuator Fault-Tolerance in Economic MPC for Nonlinear Process Plants [★]

Brage Rugstad Knudsen

[*] *Department of Engineering Cybernetics, Norwegian University of Science and Technology, N-7491 Trondheim, Norway (e-mail: brage.knudsen@itk.ntnu.no).*

Abstract:
This paper presents a scheme for proactive accommodation of incipient actuator faults in nonlinear process plants operated with economic model predictive control (EMPC). The control scheme implements a switching from nominal economic operations to a safe-transition mode when receiving a warning about an incipient fault in one of the actuators, thereby ensuring that the plant is proactively steered to a steady-state point where the suspect control actuator is inactive. Upon reaching this safe steady-state point, the faulty actuator can be safely disconnected and repaired without shutting down the plant, before the controller subsequently resumes nominal economic operation. To steer the plant to the safe steady-state point, we impose an ℓ_1 penalty function in order to achieve dead-beat control and reach the steady state in finite time. We provide a lower bound on the penalty parameter to ensure exactness of the penalty function, and analyze stability and convergence properties of the proactive fault-tolerant EMPC scheme. We demonstrate application of the proposed scheme on a non-isothermal continuously stirred tank reactor.

Keywords: Fault-tolerant MPC, Economic Optimization, Process Plants, Exact penalty functions

1. INTRODUCTION

The ability to retain safe and fault-free operations while optimizing the process economics is of prime importance in process control. Faults in actuators, sensors and components may be detrimental for product quality, in addition to being potentially dangerous for process operations, and should thus be addressed in conjunction with optimization of the process economics. Currently, the trend in dynamic economic optimization of process plants is the development of economic model predictive control (EMPC) schemes, e.g. Rawlings and Amrit (2009); Angeli et al. (2012), seeking to directly optimize the plant economics in a receding horizon manner and thereby omit the traditional hierarchical separation of steady-state real-time optimization (RTO) and set-point tracking MPC. At the same time, by being an optimal-control scheme solved online, MPC is a suitable controller in terms of directly adapting to faults in the system. Consequently, an attractive approach for integrating fault tolerance and economic receding-horizon control is to develop fault-tolerant economic MPC (FTEMPC) schemes.

In this paper, we present a *proactive* FTEMPC scheme for handling incipient actuator faults in nonlinear multiple-input process plants. A proactive fault-tolerant control (FTC) scheme seeks to detect and accommodate slowly degradation of performance or suspicious process in order to minimize negative impact on the plant if the incipient fault develops into a critical fault. Reactive approaches, on the other hand, rely on reconfiguration of the controller after the fault occurs. In this context, it is important to emphasize that proactive FTC schemes can only complement and not replace a reactive scheme capable of handling any type of (abrupt) faults in the control system. Yet, there are fault scenarios where a reactive approach may fail. If an MPC controller operates the plant close to the feasible-region boundary to maximize profit, or at an unstable steady state to for instance avoid high temperatures in an exothermic reactor (Mhaskar et al., 2008), then a sudden dropout of an actuator may shrink the feasible region of the MPC controller, or reduce the controllability of the remaining of the $m-1$ actuators, such that the controller is unable to reactively steer the plant to a safe region. Proactive FTC schemes are also suitable for controlling plants in a safety mode during inspection or replacement of suspicious or faulty actuators, or during scheduled maintenance.

An essential property of proactive FTMPC schemes is to allow plants to operate in nominal mode until a fault detection and isolation unit (FDI) sends a warning about an incipient fault. Such fault diagnosis can be obtained through parameter estimation or dedicated observer schemes, see e.g. Blanke et al. (2006). Using these methods to detect incipient faults require that the threshold values used for defining a fault event in the associated fault-detection filters are set sufficiently high to warrant early warning.

[★] The author gratefully acknowledge support from NFR grant 228460/030 and from Cybernetica AS.

Incipient fault detection may also be approached with probabilistic methods based on Markov or Bayesian analysis, see e.g. Salfner (2007). Upon receiving the warning about an incipient actuator fault, the objective of the proactive FTC scheme is to force the plant inside a region of operation or to a state where stability can be guaranteed without input from the faulty actuator. Lao et al. (2013) develop a proactive FTMPC scheme with set-point tracking using Lyapunov-based MPC, assuming exact knowledge of the time of an upcoming fault. The difficulty of this approach lies in the ability to predict when the faulty actuator will be rendered useless, the need to predesign stabilizing (Lyapunov) controllers, and that the time required to reach the safety region will depend on design and tuning of these controllers. Knudsen et al. (2016) design a proactive FTEMPC scheme for linear systems by imposing the maximum controlled invariant set with the faulty actuator inactive as a polytopic safety set, and apply an exact penalty function to steer the system inside this set in minimum time. Proactive FTMPC schemes may also be put in context of safe-parking techniques for process plants, see e.g. Gandhi and Mhaskar (2008). These methods are, however, reactive FTC approaches.

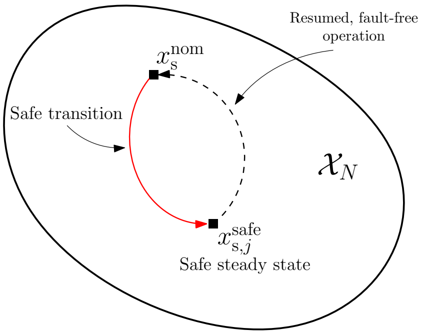


Fig. 1. Schematic illustration of the proposed proactive FTEMPC scheme.

In this paper, we extend the approach in Knudsen et al. (2016) to nonlinear process plants. In particular, we use an exact penalty function to steer the system from a nominal economic steady-state to a safe steady-state point as illustrated in Fig. 1, where the suspect control actuator can be repaired before resuming economic operations. The remainder of the paper is organized as follows: In Section 2 we present the problem formulation and set-up of the proposed proactive FTEMPC scheme. Section 3 contains analysis of stability properties of the control system. In Section 4 we demonstrate application of the proposed scheme on a non-isothermal continuously stirred tank reactor, while Section 5 ends the paper with concluding remarks.

2. PROBLEM STATEMENT

We consider nonlinear discrete-time models

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

where $x_k \in \mathbb{X} \subseteq \mathbb{R}^n$ is the state, and where $u_k \in \mathbb{U} \subseteq \mathbb{R}^m$ with $m > 1$, is the input. The operation of the plant is subject to pointwise state and input constraints,

$$(x_k, u_k) \in \mathbb{Z} \subseteq \mathbb{X} \times \mathbb{U}, \tag{2}$$

which may be both physical, economical and safety related constraints. The set $\mathbb{Z}$ is assumed compact and time invariant. We denote $i = 1, \dots n$ as index for the state vector x_k, and $k \in \mathbb{I}_{[a,b]}$ as discrete time index where $\mathbb{I}$ is the set of integers on the interval $[a, b]$. We assume that the economic objective of the process (1) is described by a stage-cost $l(x, u)$, which is optimized on a receding horizon by solving at each sampling time an open-loop dynamic optimization problem

$$V_N^{\text{nom}}(x) = \min \sum_{k=0}^{N-1} l(x_k, u_k) \tag{3a}$$

$$\text{s.t.} \quad x_{k+1} = f(x_k, u_k), \qquad k \in \mathbb{I}_{[0,N-1]}, \tag{3b}$$

$$x_0 = x, \tag{3c}$$

$$(x_k, u_k) \in \mathbb{Z}, \qquad k \in \mathbb{I}_{[0,N-1]}, \tag{3d}$$

$$x_N = x_{\text{s}}^{\text{nom}}. \tag{3e}$$

In (3c), x is the measured or estimated state of the plant. According to the conventional MPC policy, only the first element of the optimal control sequence $\mathbf{u}^*$ is applied, with reoptimization of (3) at the next sampling time when new measurements are available. In (3), we add a terminal equality constraint $x_N = x_{\text{s}}^{\text{nom}}$ defined by the solution to the economic steady-state problem

$$l(x_{\text{s}}^{\text{nom}}, u_{\text{s}}^{\text{nom}}) = \min\{l(x, u) |\ x = f(x, u), (x, u) \in \mathbb{Z}\}. \tag{4}$$

Let $\mathbf{u} = (u_0, u_1, \dots, u_{N-1})$ denote a feasible input sequence for (3). The set $\mathcal{X}_N$ of admissible states for (3) is obtained by projecting onto $\mathbb{R}^n$ the set of admissible inputs and initial states $\mathcal{Z}_N^{\text{nom}} = \{(x, \mathbf{u}) \mid \exists\ x_1, \dots, x_N$ satisfying (3b)–(3e) $\}$. Solving (3) in the described receding horizon manner defines an implicit feedback control law

$$u^{\text{nom}}(x) := u_0^*, \qquad x \in \mathcal{X}_N. \tag{5}$$

Directly applying the proactive FTEMPC approach in Knudsen et al. (2016) to the system (1)–(2) involves computing controlled invariant sets for a nonlinear control system. This is nontrivial, although some approaches exit. Instead we utilize the property that a steady-state point as defined by (4) is controlled invariant with the implicit feedback law (5) (Blanchini, 1999). In particular, to compute a *safe*, economic steady-state point $x_{\text{s},j}^{\text{safe}}$ for an incipient fault in actuator u_j, we can solve the modified steady-state problem

$$\min\{l(x, u) \mid x = f(x, u), (x, u) \in \mathbb{Z}, u_j = 0\}. \tag{6}$$

The problem (6) must be solved (offline) for each set of actuator fault scenarios. For simplicity, however, we restrict our study to single actuator faults. We further make the following assumption:

Assumption 1. The plant described by (1)–(2) admits a unique steady state pair $(x_{\text{s},j}^{\text{safe}}, u_{\text{s},j}^{\text{safe}})$ with $u_j = 0$.

At time t^{fw}, when an FDI unit sends warning about an incipient fault in actuator j, a switching logic is triggered to switch from solving the nominal EMPC problem (3) to a safe-transition mode. For this safe-transition mode, we seek to steer the system to $x_{\text{s},j}^{\text{safe}}$ by a dead-beat control policy, that is, by a control policy such that the system is steered to the desired operating point in a minimum number of time steps and kept there, see e.g. Rao and Rawlings (2000) or Keerthi and Gilbert (1988). To this end, we replace $x_{\text{s}}^{\text{nom}}$ in the terminal equality constraint (3e) with $x_{\text{s},j}^{\text{safe}}$, and add an ℓ_1 penalty term with a penalty parameter $\mu > 0$ to the economic stage cost $l(x, u)$,

$$l^{\text{safe}}(x, u) := l(x, u) + \mu \left| x - x_{\text{s},j}^{\text{safe}} \right|_1. \tag{7}$$

By introducing vectors $(\epsilon_k^+, \epsilon_k^-) \in \mathbb{R}^n$ of nonnegative slack variables, we can reformulate the nonsmooth ℓ_1 norm in (7) to a smooth equivalent formulation. Consequently, at time t^{fw} when the EMPC controller receives a warning about an incipient fault in actuator j, we switch from solving the nominal EMPC problem (3) to the following NLP safe-transition MPC problem:

$$
\begin{aligned}
V_N^{\text{safe}}(x) = \min & \sum_{k=0}^{N-1} \left(l(x_k, u_k) + \mu \sum_{i=1}^{n} \epsilon_{ik}^+ + \epsilon_{ik}^- \right) && && \text{(8a)}\\
\text{s.t.} \quad & x_{k+1} = f(x_k, u_k), && k \in \mathbb{I}_{[0,N-1]}, && \text{(8b)}\\
& x_0 = x, && && \text{(8c)}\\
& (x_k, u_k) \in \mathbb{Z}, && k \in \mathbb{I}_{[0,N-1]}, && \text{(8d)}\\
& x_k - x_{\text{s},j}^{\text{safe}} = \epsilon_k^+ - \epsilon_k^-, && k \in \mathbb{I}_{[0,N-1]}, && \text{(8e)}\\
& \epsilon_{k+1}^+ \leq \epsilon_k^+, && k \in \mathbb{I}_{[0,N-2]}, && \text{(8f)}\\
& \epsilon_{k+1}^- \leq \epsilon_k^-, && k \in \mathbb{I}_{[0,N-2]}, && \text{(8g)}\\
& \epsilon_k^+, \epsilon_k^- \geq 0, && && \text{(8h)}\\
& x_N = x_{\text{s},j}^{\text{safe}}. && && \text{(8i)}
\end{aligned}
$$

Solving (8) in the aforementioned receding horizon manner defines an implicit feedback control law

$$u^{\text{safe}}(x) := \bar{u}_0^*, \qquad \forall x \in \mathcal{X}_N. \tag{9}$$

where $\bar{\mathbf{u}}^*$ is the optimal control sequence obtained by solving (8). For (8), we invoke the following reachability assumption.

Assumption 2. The system can be steered to $x_{s,j}^{\text{safe}}$ within N timesteps with the remaining actuation capacity available at time t^{fw}.

In addition to a sufficiently large N, this assumption also implies that the onset of the incipient fault is detected early, requiring the threshold values used in the fault-detection filter to be sufficiently high, such that there is enough remaining actuator capacity to steer the system to the safe park $x_{\text{s},j}^{\text{safe}}$ before eventual failure of the faulty actuator.

Upon reaching the steady state $x_{\text{s},j}^{\text{safe}}$, we have steered the plant to a positively invariant set for the closed-loop system $x_{k+1} = f(x_k, u^{\text{safe}}(x))$, defined by singleton, at which the plant remains safe despite a dropout of actuator j. As such, the controller can safely continue economic operation of the process during inspection and replacement of the faulty actuator. We thereby prevent a shut down of the plant to recover from an incipient fault, reducing costs associated with false fault alarms. Observe that at most one slack variable will be strictly positive for each corresponding pair $(\epsilon_{ik}^+, \epsilon_{ik}^-)$. Furthermore, note that the initial condition (8c) at sample time t^{fw} when we switch to solving (8) in the EMPC controller will be the state measured or estimated from applying the solution to (3) at time $t^{\text{fw}} - 1$ to the plant. As there are no differences between the two EMPC problems except from the ℓ_1 penalty term and the terminal condition, there are no jumps in the states at the time of switching between nominal and safe-transition EMPC mode.

By imposing ℓ_1 as opposed to a quadratic penalty, we can ensure that EMPC controller steers the plant to $x_{\text{s},j}^{\text{safe}}$ in finite time by a dead-beat control policy (Rao and Rawlings, 2000; Keerthi and Gilbert, 1988). Moreover, the ℓ_1 penalty term makes it possible to define an exact penalty function with an associated lower bound on μ.

Proposition 3. Suppose that f and l are continuous functions, and that the LICQ conditions hold at a strict local solution $(x_{\text{s},j}^{\text{safe}}, u_{\text{s}}^*)$ to the steady-state problem

$$\min\{l(x,u) \mid x = f(x,u), (x,u) \in \mathbb{Z}, x = x_{\text{s},j}^{\text{safe}}\}, \tag{10}$$

with Lagrange multipliers ν^*. Then the reformulated ℓ_1 penalty function in (8) will be exact if $\mu > \mu^*$, where $\mu^* = ||\nu^*||_\infty$.

Proof. It is well known that for the ℓ_1 penalty function of an NLP to be exact, we must have $\mu > ||\nu^*||_\infty$, where ν^* are Lagrange multipliers of the NLP, in which stationary points of the penalty function are either KKT points of the corresponding NLP or infeasible stationary points, i.e. with $(\epsilon_k^+, \epsilon_k^-) > 0$. See e.g. Conn et al. (2000, Ch. 14.5). For a solution to (8) to be feasible for the corresponding hard-constrained problem, it must satisfy $x_k = x_{\text{s},j}^{\text{safe}}$ for all $k = 0, \ldots N$. This problem is equivalent with solving N steady-state problems (4) with fixed optimal state vector $x_{\text{s},j}^{\text{safe}}$, i.e. as stated by (10). Assuming that the LICQ condition holds at the solution (10) ensures uniqueness of ν^*. □

At time t^{fw} when the safe-transition MPC problem is invoked, the solution to (8) will clearly be infeasible for the corresponding hard-constrained problem, i.e. giving a solution with $(\epsilon_k^+, \epsilon_k^-) > 0$ up to some time index $\bar{k} \in \mathbb{I}_{[1,N-1]}$. By Proposition 3, the only time the solutions to the soft-constrained problem (8) and the corresponding hard-constrained problem will coincide is when $x_0 = x_{\text{s},j}^{\text{safe}}$. Exactness of the penalty function will, however, ensure a locally "least-infeasible" solution, see Conn et al. (2000, Ch. 14.5).

If the penalty parameter μ is sufficiently large, then the solution to (10) is a solution to

$$\min\{l(x,u) + \mu \left| x - x_{\text{s},j}^{\text{safe}} \right| \; \Big| \; x = f(x,u), (x,u) \in \mathbb{Z}\}, \tag{11}$$

which is the steady-state problem corresponding to (8). By assumption, the solution to (6) yields a unique steady-state point $(x_{\text{s},j}^{\text{safe}}, u_{\text{s},j}^{\text{safe}})$. Consequently, $u_{\text{s}}^* = u_{\text{s},j}^{\text{safe}}$ must be the solution to (10), and hence also solve the steady-state problem (11). Note that (11) can be reformulated to a smooth NLP in the same way as (8).

The lower bound on μ provides a means for tuning the EMPC controller by providing a threshold value to ensure the desired property of exactness of the penalty function, while it also prevents numerical issues associated with setting μ too large. By using Proposition 3, we can solve (10) to compute $||\nu^*||_\infty$ and set μ only marginally larger than this value. This procedure circumvents the tuning challenges associated with a quadratic cost in order to ensure a sufficiently fast convergence to the safe steady-state $x_{\text{s},j}^{\text{safe}}$. A drawback of the ℓ_1 penalty is the increase in problem size caused by reformulation with slack variables. Generally, however, efficient NLP solvers such as IPOPT (Wächter and Biegler, 2005) are able to exploit sparsity structures in the NLP, and thereby limit any additional computational burden caused by the increase in problem size.

Remark 4. If the steady-state point $(x_{\mathrm{s},j}^{\mathrm{safe}}, u_{\mathrm{s},j}^{\mathrm{safe}})$ obtained by solving (6) is non-unique, that is, there exists steady-state pairs $(x_{\mathrm{s},j}^{\mathrm{safe}}, \tilde{u}_{\mathrm{s},j})$ with $\tilde{u}_{\mathrm{s},j} \neq u_{\mathrm{s},j}^{\mathrm{safe}}$, then the solution to (10) may yield a steady state with lower cost than $l(x_{\mathrm{s},j}^{\mathrm{safe}}, u_{\mathrm{s},j}^{\mathrm{safe}})$ and $u_{\mathrm{s}}^* \neq u_{\mathrm{s},j}^{\mathrm{safe}}$.

Remark 5. In some applications, it may be desirable to tighten the bounds given by $\mathbb{Z}$ on the states and healthy inputs in a safety mode. In this case the lower bound on μ given by Proposition 3 is no longer sufficient to ensure exactness of the penalty function in (8).

3. STABILITY ANALYSIS

In the following section, we analyze stability and convergence properties of the proposed proactive FTEMPC scheme. To this end, we need the definition of dissipativity.

Definition 6. (Angeli et al., 2012) The system (1) is dissipative with respect to the supply rate $s : \mathbb{X} \times \mathbb{U} \mapsto \mathbb{R}$ if there exists a storage function $\lambda : \mathbb{X} \mapsto \mathbb{R}$ such that

$$\lambda(f(x,u)) - \lambda(x) \leq s(x,u), \tag{12}$$

for all $(x,u) \in \mathbb{Z}$. If there exists a positive definite function[1] $\rho : \mathbb{X} \mapsto \mathbb{R}$ such that

$$\lambda(f(x,u)) - \lambda(x) \leq s(x,u) - \rho(x), \tag{13}$$

then the system is said to be strictly dissipative.

Angeli et al. (2012) prove that if the system (1) is weakly controllable and strictly dissipative with respect to the supply rate

$$s(x,u) = l(x,u) - l(x_{\mathrm{s}}^{\mathrm{nom}}, u_{\mathrm{s}}^{\mathrm{nom}}), \tag{14}$$

then x_s^{nom} is an asymptotically stable steady-state point of the EMPC scheme defined by (3) and (5), provided certain technical assumptions hold, see Angeli et al. (2012). Hence, we focus on stability properties of the safe-transition EMPC scheme defined by (8) and (9). In particular, we have the following nominal stability result (perfect model and no disturbances):

Theorem 7. Suppose that $\mu > \mu^*$ such that the ℓ_1 penalty function (8a) is exact, and that the system (1) is controlled with the EMPC scheme defined by (8) and (9). Then the following holds:

(i) If (8) is feasible at time t^{fw} for an initial condition $x \in \mathcal{X}_N$, it will remain feasible for all nonnegative times, and steer the state to $x_{\mathrm{s},j}^{\mathrm{safe}}$ in a minimum number of time-steps $\bar{k}$, where $\bar{k} = \{k \in \mathbb{I}_{[1,N-1]} \mid (\epsilon_k^{+*}, \epsilon_k^{-*}) = 0,\ \forall k > \bar{k}\}$ with $(\epsilon_k^{+*}, \epsilon_k^{-*})$ as optimal slack vectors computed at time t^{fw}.

(ii) If (i) holds, $x_{\mathrm{s},j}^{\mathrm{safe}}$ is in the interior of $\mathcal{X}_N$, and the system (1) is strictly dissipative with respect to the supply rate

$$s(x,u) = l^{\mathrm{safe}}(x,u) - l^{\mathrm{safe}}(x_{\mathrm{s},j}^{\mathrm{safe}}, u_{\mathrm{s},j}^{\mathrm{safe}}), \tag{15}$$

then $x_{\mathrm{s},j}^{\mathrm{safe}}$ is an asymptotically stable steady-state point of the closed-loop system $x_{k+1} = f(x_k, u_{\mathrm{s}}^{\mathrm{safe}}(x))$ with region of attraction $\mathcal{X}_N$.

Proof. Let $\{(\epsilon_0^+, \epsilon_0^-), (\epsilon_1^+, \epsilon_1^-), \ldots, (\epsilon_{\bar{k}}^+, \epsilon_{\bar{k}}^-), 0, \ldots, 0\}$ be a sequence of feasible slack vectors computed at sampling time t^{fw}, for some $\bar{k} \in \mathbb{I}_{[1,N-1]}$. By applying the first element $\bar{u}_0^*$ of the optimal control sequence $\bar{\mathbf{u}}^*$ to the plant, then at sampling time $t^{\mathrm{fw}} + 1$ the sequence of slack vectors shifted one step ahead, i.e. $\{(\epsilon_1^+, \epsilon_1^-), \ldots, (\epsilon_{\bar{k}}^+, \epsilon_{\bar{k}}^-), 0, 0 \ldots, 0\}$, will be feasible for (8) with initial condition $f(x, \bar{u}_0^*)$, due to the terminal equality constraint (8i). Moreover, due the same terminal equality constraint, the control sequence $\{\bar{u}_1^*, \bar{u}_2^*, \ldots, \bar{u}_{N-1}^*, u_{\mathrm{s},j}^{\mathrm{safe}}\}$ will be feasible. Feasibility for all nonnegative timesteps hence follows by induction.

Provided that the ℓ_1 penalty function (8a) is exact, then a solution to the soft-constrained problem (8) will either satisfy the KKT conditions for the hard-constrained problem, or it will be a locally least infeasible solution. The latter means that *locally* to a feasible solution to the hard-constrained problem, that is, a solution satisfying $x_k = x_{\mathrm{s},j}^{\mathrm{safe}}, \forall k \in \mathbb{I}_{[0,N]}$, the pairs of optimal slack vectors $(\epsilon_k^{+*}, \epsilon_k^{-*})$ will be nonzero only for those $k \in \mathbb{I}_{[0,N-1]}$ for which there does not exist a feasible input sequence such that $x_k = x_{\mathrm{s},j}^{\mathrm{safe}}$. Since $(\epsilon_k^{+*}, \epsilon_k^{-*})$ computed at sampling time t^{fw} shifted one step ahead will be feasible for (8) at time $t^{\mathrm{fw}} + 1$, and that this solution provides feasibility for one more of the softened constraints, then exactness of the penalty function and invariance of the steady state $x_{\mathrm{s},j}^{\mathrm{safe}}$, enforced as a terminal equality constraint, yield a solution to (8) at time $t^{\mathrm{fw}} + 1$ with at most $\bar{k} - 1$ nonzero slack vectors. Consequently, in the nominal case, the EMPC scheme (8)–(9) will ensure one less nonzero slack vector for each timestep, and hence steer the state from $x \in \mathcal{X}_N$ to $x_{\mathrm{s},j}^{\mathrm{safe}}$ in a locally minimum number of timesteps. This proves part (i).

Feasibility of (8) at time t^{fw} ensures that $V_N^{\mathrm{safe}}(x)$ is finite, and hence that the cost of steering x to $x_{\mathrm{s},j}^{\mathrm{safe}}$ is finite. Part (ii) of the theorem, asymptotic stability of $x_{\mathrm{s},j}^{\mathrm{safe}}$ for the closed-loop system $x_{k+1} = f(x_k, u_{\mathrm{s}}^{\mathrm{safe}}(x))$, then follows directly from Theorem 2 in Angeli et al. (2012). □

We emphasize that the solution provided by the exact penalty function (8) only gives *local* minimum-time solution due to the nonconvexity of the NLP. Consequently, there may exist other local solutions to (8) for initial conditions $x \in \mathcal{X}_N$ that are "'less infeasible"' with respect to the softened constraints, and hence steers the plant to $x_{\mathrm{s},j}^{\mathrm{safe}}$ in fewer timesteps.

If the NLP (8) is infeasible at time t^{fw}, then either some emergency or safety mode must be activated, for instance to stop all feeding of reactants or to set the cooling to its maximum level. On the other hand, the EMPC controller should in this case probably be redesigned in terms of tightening the constraints or increasing the prediction horizon. A property under investigation is whether an *exact* penalty as in (8) together with certain additional assumptions for the system (1) can be used to formulate a sufficient condition for strict dissipativity with respect to the supply rate (15). Yet, however, the storage function $\lambda(x)$ must be computed to verify strict dissipativity, which in general is difficult. One approach is using sum-of-squares programming, see e.g. Faulwasser et al. (2014).

Remark 8. The proactive FTEMPC formulation (8) inherits the numerical difficulties associated with a terminal

[1] A continuous function $\rho(x)$ is said to be positive definite with respect to some point $x_s \in \mathbb{X}$ if $\rho(x_{\mathrm{s}}) > 0, \forall x \neq x_{\mathrm{s}}$ and $\rho(x_{\mathrm{s}}) = 0$.

equality constraint. From a stability perspective, however, this terminal equality constraint is important, although EMPC schemes without this terminal constraint exist.

4. NON-ISOTHERMAL CSTR

To illustrate the proposed proactive FTEMPC scheme, we consider a non-isothermal continuously stirred tank reactor (CSTR) problem, adopted from Ellis et al. (2014). In the CSTR, an elementary exothermic second-order reaction takes place, converting a reactant A to a desired product B, with a cooling jacket providing or removing heat to and from the reactor. The temperature and composition of the CSTR are assumed to be uniform. The reactant is fed to the reactor through a feedstock stream with concentration C_{A0}, with given flow rate F and temperature T_0. The resultant CSTR model reads

$$\frac{dC_A}{dt} = \frac{F}{V_{\mathrm{R}}}\left(C_{A0} - C_A\right) - k_0 e^{-\frac{E}{RT}} C_A^2, \tag{16a}$$

$$\frac{dT}{dt} = \frac{F}{V_{\mathrm{R}}}(T_0 - T) - \frac{\Delta H k_0}{\rho_{\mathrm{R}} C_{\mathrm{p}}} e^{-\frac{E}{RT}} C_A^2 + \frac{Q}{\rho_{\mathrm{R}} C_{\mathrm{p}} V_{\mathrm{R}}}. \tag{16b}$$

We consider the CSTR with two manipulated inputs, the inlet concentration, $u_1 = C_{A0}$, with a maximum concentration of 7.5 kmol/m^3, and the jacket heat rate, $u_2 = Q$, with available control energy $|Q| \leq 50 \times 10^3$ kJ/h. The stage cost is set equal to the production rate of the desired product C_A, i.e.

$$l(x, u) = -k_0 e^{-\frac{E}{RT}} C_A^2. \tag{17}$$

Numerical values and descriptions of the process parameters in (16) are given in Table 1.

Table 1. Process parameters of CSTR.

Par.	Description	Value	Unit
F	Feed flow rate	5.0	m^3/h
T_0	Feed temperature	300	K
k_0	Pre-exponential rate factor	8.46×10^6	1/kmolh
V_{R}	Reactor fluid volume	1.0	m^3
ρ_{R}	Density	1000	kg/m^3
R	Gas constant	8.314	kJ/kmolK
E	Activation energy	5×10^4	kJ/kmol
ΔH	Reaction enthalpy change	-1.16×10^4	kJ/kmol
C_{p}	Heat capacity	0.231	kJ/kgK

The CSTR model (16) is discretized in time using the backward Euler method. We solve the NLP MPC problems using IPOPT, while the steady-state problems are solved to global optimality using BARON. All problems are implemented in GAMS. We initialize the system at nominal optimal steady-state $x_{\mathrm{s}}^{\mathrm{nom}} = (0.142, 712.8)$, where $x_1 = C_A$ and $x_2 = T$, and assume that the control system receives a warning about an incipient fault in actuator $u_2 = Q$ at sampling time $t^{\mathrm{fw}} = 0$. We apply a prediction horizon of $N = 100$ and timestep of 0.002 hours. Computing (6) for the CSTR model (16)–(17) gives the safe steady-state point $x_{\mathrm{s},j}^{\mathrm{safe}} = (0.188, 667.2)$, while computing (10) gives the lower bound $\mu^* = 5.27$ on the ℓ_1 penalty.

To highlight the importance of adding the ℓ_1 penalty term in (8a), we compare in Fig. 2 the open-loop response at time t^{fw} and the corresponding closed-loop response solving (8), with the corresponding response *without* the ℓ_1 term, but with the terminal equality constraint (8i).

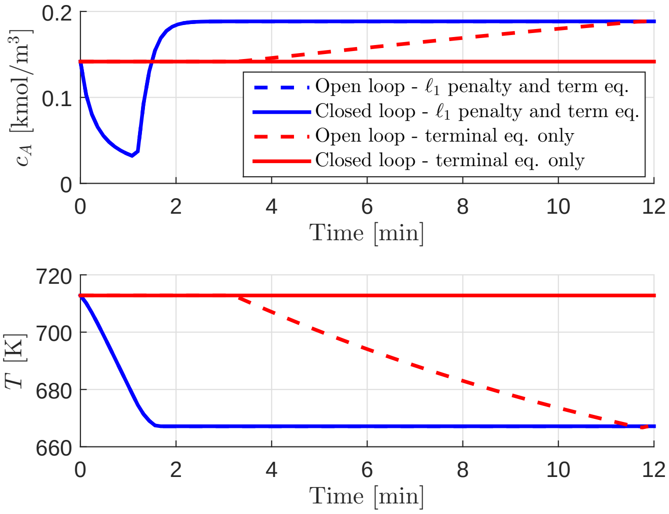
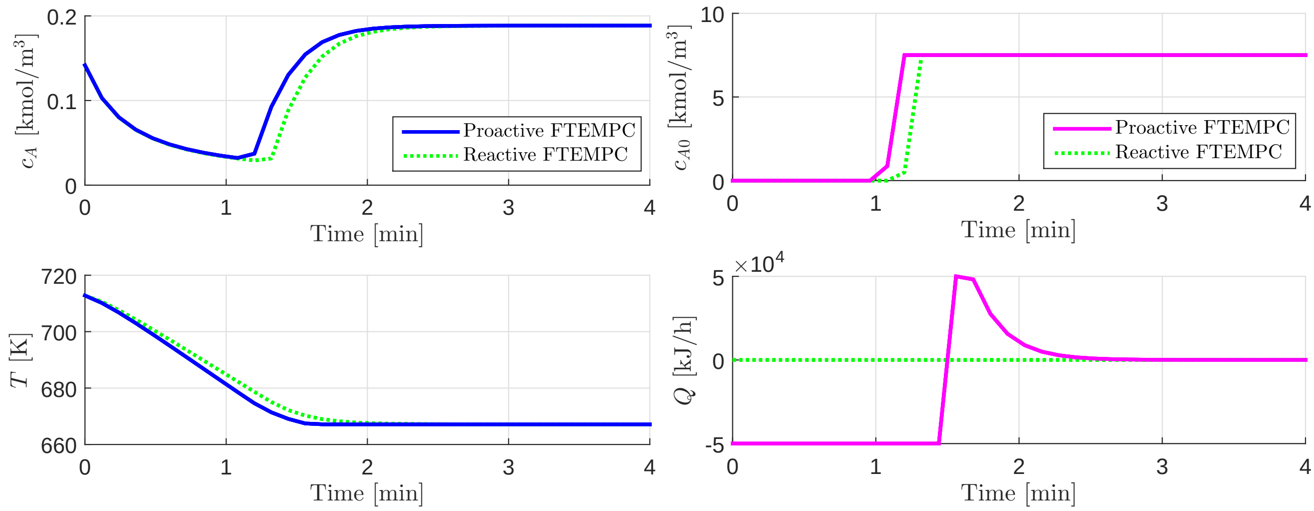


Fig. 2. Comparison of open-loop and closed-loop response with (blue) and without (red) the ℓ_1 penalty in the objective function (8a) in the safe-transition MPC problem (8). Observe that open-loop and closed-loop response with the ℓ_1 penalty coincide.

Solving (8) with the ℓ_1 penalty steers the state to $x_{\mathrm{s},j}^{\mathrm{safe}}$ in finite time, where the open-loop and closed-loop response are indistinguishable. Without the ℓ_1 penalty, $x_{\mathrm{s},j}^{\mathrm{safe}}$ is a suboptimal steady-state for the nominal, fault-free system. The open-loop response can be seen to exhibit a turnpike behavior, see e.g. Rawlings and Amrit (2009), in which the plant spends as much time as possible close to the optimal steady state, and is steered to $x_{\mathrm{s},j}^{\mathrm{safe}}$ exactly at the end of the horizon. In closed-loop, the plant therefore remains at the optimal economic steady state $x_{\mathrm{s}}^{\mathrm{nom}}$, as seen by the solid red line in Fig. 2, at which it will remain until the faulty actuator ultimately fails.

In Fig. 3 we compare the proposed proactive FTEMPC scheme with a simulated *reactive* approach. For the reactive scheme, we assume that no proactive manipulation of inputs are performed upon receiving warning about the incipient fault in $u_2 = Q$, and as such that switching to the safe-transition EMPC problem (8) is triggered first when the actuator eventually becomes useless. In this reactive scheme, the constraints and model in the EMPC problem are updated to account for the failure of the actuator, i.e. Q is set to 0.

To directly compare the evolution of states and inputs for the proactive and reactive approach, we simulate the reactive approach from the same initial time and state as the proactive approach, but consequently with $u_2 = Q = 0$. That is, we *shift* backwards to time $t^{\mathrm{fw}} = 0$ the time when the fault actually occurs, which is the time when the reactive approach invokes (8). We assume that the actual failure time of Q is beyond the simulation time of the proactive approach, as once the plant reaches $x_{\mathrm{s},j}^{\mathrm{safe}}$ the fault should by design not impact the control of the plant. Comparing in Fig. 3 the closed-loop response of these two approaches, it can be seen that the proactive scheme requires less time than the reactive approach to steer the plant to $x_{\mathrm{s},j}^{\mathrm{safe}}$. In particular, the reactive approach requires 42 timesteps to reach $x_{\mathrm{s},j}^{\mathrm{safe}}$, while in comparison the proactive approach requires 33 timesteps. In Fig. 3(b),



(a) States.

(b) Manipulated variables.

Fig. 3. Comparison of the proposed proactive FTEMPC scheme (solid lines) with a corresponding reactive scheme (dashed lines).

it is seen that both approaches stop the feed C_{A0} for some time to reduce the concentration and temperature, while the proactive approach actively uses the jacket heat rate Q to quicker lower the temperature T, and thereby reduce the time to reach $x_{s,j}^{\text{safe}}$. Observe that in this example, the reactive FTMPC approach also retain the necessary controllability to steer the plant to $x_{s,j}^{\text{safe}}$ with only the feed C_{A0} as remaining manipulated variable.

5. CONCLUSIONS

In this paper, a proactive FTEMPC scheme is constructed with the objective of ensuring that the plant is steered to a safe, recoverable steady state at the detection of an incipient actuator fault. As illustrated through simulations of a CSTR, the proactive scheme reduces the time required to steer the plant to a region of operation where the fault can be improved, thereby reducing the overall time spent to improve the fault before the controller can resume nominal economic operations. The proposed proactive FTEMPC scheme may thus reduce costs of handling incipient actuator faults, prevent unnecessary plant shut downs due to false false alarms, and facilitate preventive maintenance. Thus, the scheme may serve as a complement to reactive fault-tolerant control schemes able to handle any type of abrupt faults in the system. Future work includes incorporating reduction of actuation capacity during the time from warning of an incipient fault to failure of an actuator.

REFERENCES

Angeli, D., Amrit, R., and Rawlings, J.B. (2012). On average performance and stability of economic model predictive control. *IEEE Trans. Autom. Control*, 57(7), 1615–1626.

Blanchini, F. (1999). Set invariance in control. *Automatica*, 35(11), 1747–1767.

Blanke, M., Kinnaert, M., Lunze, J., and Staroswiecki, M. (2006). *Diagnosis and Fault-Tolerant Control*. Springer.

Conn, A., Gould, N., and Toint, P. (2000). *Trust Region Methods*. SIAM, Philadelpia.

Ellis, M., Durand, H., and Christofides, P.D. (2014). A tutorial review of economic model predictive control methods. *J. Process Contr.*, 24(8), 1156–1178.

Faulwasser, T., Korda, M., Jones, C., and Bonvin, D. (2014). Turnpike and dissipativity properties in dynamic real-time optimization and economic MPC. In *Proc. of the IEEE Conf. Decision Control*, 2734–2739.

Gandhi, R. and Mhaskar, P. (2008). Safe-Parking of nonlinear process systems. *Comput. Chem. Eng.*, 32(9), 2113–2122.

Keerthi, S.S. and Gilbert, E.G. (1988). Optimal infinite-horizon feedback laws for a general class of constrained discrete-time systems: Stability and moving-horizon approximations. *J. Optim. Theory. Appl.*, 57(2), 265–293.

Knudsen, B.R., Brusevold, J.H., and Foss, B. (2016). An exact penalty-function approach to proactive fault-tolerant economic MPC. In *Prep. of Eur. Control Conf.* Aalborg, Denmark.

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

Mhaskar, P., McFall, C., Gani, A., Christofides, P.D., and Davis, J.F. (2008). Isolation and handling of actuator faults in nonlinear systems. *Automatica*, 44(1), 53–62.

Rao, C.V. and Rawlings, J.B. (2000). Linear programming and model predictive control. *J. Process Control*, 10(2), 283–289.

Rawlings, J.B. and Amrit, R. (2009). Optimizing process economic performance using model predictive control. In L. Magni, D.M. Raimondo, and F. Allgwer (eds.), *Nonlinear Model Predictive Control*, volume 384 of *Lect. Notes. Contr. Inf.*, 119–138. Springer Berlin Heidelberg.

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.