An exact penalty-function approach to proactive fault-tolerant economic MPC

Brage Rugstad Knudsen, Jon H. Brusevold and Bjarne Foss

***Abstract*— This paper presents a fault-tolerant economic model predictive control scheme for proactive handling of incipient actuator faults. The scheme applies an ℓ_1 exact penalty function with a set of switching rules in order to steer the system by a minimum-time approach inside a controlled invariant set where stability of the system can be preserved during loss of actuation from the faulty actuator. We consider the approach for linear control systems, thereby allowing computation of a lower bound for the penalty parameter to ensure exactness of the penalty function. We prove nominal asymptotic stability of the modes of the proposed model predictive control scheme, and illustrate the approach by a numerical example.**

I. INTRODUCTION

Fault tolerance in optimal control of dynamic systems is important both for safety and economic optimality of operations. A structured and effective fault-tolerant control (FTC) scheme can improve the reliability and continuity of system operations, both for safety-critical processes and for chemical production and manufacturing. Dynamic optimization-based control, on the other hand, requires the ability to handle complex systems with hard control constraints and many inputs and outputs. This has caused model predictive control (MPC) to become a widely adopted control scheme [1]. Since MPC is an optimal-control scheme solved online, these controllers also enable direct adaptation to faults in the system [2]. Recently, there has been increased focus on economic model predictive control (EMPC) which, contrary to separated real-time optimization (RTO) and MPC, merges dynamic economic operations with the feedback properties of conventional MPC [1], [3], [4], [5]. The objective of this paper is as such to integrate actuator fault tolerance in economic MPC towards the design of efficient fault-tolerant, economically optimizing control schemes.

Reconfigurable (active) FTC methods can broadly be classified as reactive or proactive [6]. Reactive approaches basically rely on controller reconfiguration after a fault occurs, while, in comparison, a proactive scheme seeks to utilize information about an incipient fault in the system, indicated by slowly developing performance degradation, to proactively manipulate the inputs and thereby minimize negative impact of a possible future fault. In this context, it is evident that proactive FTC schemes are not intended to replace a reactive scheme capable of handling abrupt faults in the system. However, proactive (or preventive) FTC is emerging as a complement to reactive schemes, and can, if designed properly, be efficiently applied to ensure sustainable process operations, minimize down time and prevent shut-downs for certain types of faults in the system, as well as to perform scheduled maintenance.

In this paper, we develop a fault-tolerant MPC (FTMPC) scheme for handling incipient actuator faults. We choose to focus on economic MPC, in conjunction with the rapid developments of this scheme, while the approach can be extended to tracking MPC as well. The proactive FTMPC scheme assumes that a fault detection and isolation unit (FDI) is able to detect an incipient fault in one of the actuators, and provide a *conservative* estimate of a time window between the warning about an incipient fault and the likelihood of complete failure of the actuator. See [7] for an example on these types of fault-prediction schemes. To prevent possible loss of controllability and system destabilization, a proactive FTMPC scheme seeks to steer the system inside a safety region upon receiving warning about an incipient actuator fault. In [6], this is obtained by using Lyapunov-based tracking MPC, assuming that predesigned stabilizing Lyapunov-based controllers exist. Their approach, however, does not provide guarantees on the convergence rate to the safety region, as this depends on tuning of the predesigned controllers. In [8], a hybrid FTMPC scheme is developed with scenario-based safety constraints and reconfigurable control.

The novelty of this paper lies in the construction of a proactive FTMPC scheme that applies an exact penalty function to steer the state inside a controlled invariant safety set with the suspect control actuator inactive, allowing the system to retain economic operation during the time of loss of actuation, and resume nominal operations once repaired. The paper is organized as follows: In Section II we present the problem and the set-up of the proposed proactive FTMPC scheme. Section II-A outlines the computation of an exact penalty parameter, and Section III analyzes stability properties of the controllers. Section IV presents a numerical example to illustrate the proposed scheme, while Section V ends the paper with concluding remarks.

II. PROBLEM DESCRIPTION

We consider proactive fault-tolerant MPC for discrete linear time-invariant (LTI) systems,

$$x_{k+1} = Ax_k + Bu_k, \tag{1}$$

where $x_k \in \mathbb{X} \subseteq \mathbb{R}^n$ is the state, $u_k \in \mathbb{U} \subseteq \mathbb{R}^m$ with $m > 1$ is the input, and where $A \in \mathbb{R}^{n\times n}$ and $B \in \mathbb{R}^{n\times m}$. We denote $k \in \mathbb{I}_{[a,b]}$ as the discrete time index, where $\mathbb{I}$ is the set of integers on the interval $[a,b]$. During nominal operations, the

The authors are with the Department of Engineering Cybernetics, Norwegian University of Science and Technology. Corresponding author: Brage R. Knudsen (brage.knudsen@itk.ntnu.no). Support from NFR grant 228460/030 and from Cybernetica AS is gratefully acknowledged.

EMPC controller optimizes the economics of the system by solving at each sampling time t the finite-horizon optimal-control problem $P^{\text{nom}}(x)$:

$$V_N^{\text{nom}}(x) = \min \sum_{k=0}^{N-1} l(x_k, u_k) \tag{2a}$$

$$\text{s.t.} \quad x_{k+1} = Ax_k + Bu_k, \qquad k \in \mathbb{I}_{[0,N-1]} \tag{2b}$$

$$x_0 = x, \tag{2c}$$

$$(x_k, u_k) \in \mathbb{Z}^{\text{nom}}, \qquad k \in \mathbb{I}_{[0,N-1]} \tag{2d}$$

$$x_N = x_{\text{s}}^{\text{nom}}, \tag{2e}$$

where x is the current state of the system, and where the compact set

$$\mathbb{Z}^{\text{nom}} \subseteq \mathbb{X} \times \mathbb{U} \tag{3}$$

defines point-wise in time polytopic constraints on the states and inputs.

Assumption 1. The economic stage cost $l(x,u)$ is convex.

The terminal equality constraint (2e) is defined by the solution $(x_{\text{s}}^{\text{nom}}, u_{\text{s}}^{\text{nom}})$ to the steady-state problem

$$\min\{l(x,u) \mid x = Ax + Bu,\ (x,u) \in \mathbb{Z}^{\text{nom}}\}. \tag{4}$$

We assume that $(x_{\text{s}}^{\text{nom}}, u_{\text{s}}^{\text{nom}})$ uniquely solves (4) with objective value $l(x_{\text{s}}^{\text{nom}}, u_{\text{s}}^{\text{nom}})$. Operation of the system in faulty and nominal mode imposes different state and/or input constraints, as well as a modified control matrix, denoted B_j, when the fault occurs. These varying constraints give different optimal steady-state points. Let $\mathbf{u} = (u_0, u_1, \ldots, u_{N-1})$ denote a feasible input sequence for (2). The set $\mathcal{X}_N^{\text{nom}}$ of admissible states for $P^{\text{nom}}(x)$ is then obtained by projecting the set of admissible inputs and initial states $\mathbb{Z}_N^{\text{nom}} = \{(x, \mathbf{u}) \mid \exists\, x_1, \ldots, x_N$ satisfying (2b)–(2e)$\}$ onto $\mathbb{R}^n$. The system (1) may be unstable, but we make the following N-step controllability assumption.

Assumption 2. The nominal system (A,B) and the faulty system (A,B_j) are both controllable, and N is chosen sufficiently large such that all *admissible* initial states $x \in \mathcal{X}_N^{\text{nom}}$ can be steered to an admissible economic steady-state $(x_{\text{s}}, u_{\text{s}})$ within N steps while satisfying the given state and input constraints.

Assumption 2 ensures that the system can be steered from any admissible initial state x to an admissible steady-state x_{s} in N timesteps. It is important to emphasize that we assume this condition to hold for *any* admissible economic steady-state point, as the latter changes by introducing safety constraints. By the conventional MPC control law, only the first move of the optimal input sequence $\mathbf{u}^*$ from solving $P^{\text{nom}}(x)$ is applied to the system, defining an implicit feedback law $u_{\text{e}}^{\text{nom}}(x) := u_0^*$. At each sampling time t, $P^{\text{nom}}(x)$ is repeatedly reoptimized in a receding-horizon manner with the current state (2c) updated through measurements of x. We assume that the full state is measurable, i.e. we consider state feedback MPC. Note that the set $\mathcal{X}_N^{\text{nom}}$ is positive invariant due to the imposed terminal constraint (2e), i.e. $x \in \mathcal{X}_N^{\text{nom}}$ implies $(Ax + Bu_{\text{e}}^{\text{nom}}(x)) \in \mathcal{X}_N^{\text{nom}}$ [5].

The objective of this paper is to construct a proactive fault-tolerant economic MPC controller that allows continued (suboptimal) economic operations of the system in the presence of an incipient actuator fault. We consider the following fault scenario illustrated in Fig. 1. At time t_{fw}, the system is operating at the economic optimal steady state $x_{\text{s}}^{\text{nom}}$, when an FDI unit sends a fault warning (fw) indicating an incipient fault in actuator $j \in \{1 \ldots m\}$, together with a conservative estimate $t_{\text{f}} - t_{\text{fw}}$ of a time window between the warning of an incipient fault and the time when the fault is likely to occur. To prevent possible destabilization due to a future dropout of the faulty actuator, the EMPC controller must steer the system from $x_{\text{s}}^{\text{nom}}$ to a controlled invariant safety set $\mathbb{S}_j \subset \mathbb{R}^n$ containing the steady-state point $x_{\text{s},j}^{\text{safe}}$, within the time window $t_{\text{f}} - t_{\text{fw}}$. When inside this safety set, the EMPC controller can safely continue operating the system despite a dropout of actuator j. If the faulty actuator eventually fails or is taken out of action, the system should be steered from the steady state $x_{\text{s},j}^{\text{safe}}$ to a new "fault" steady state $x_{\text{s},j}^{\text{fault}}$, where the faulty actuator is repaired before resuming nominal operations.

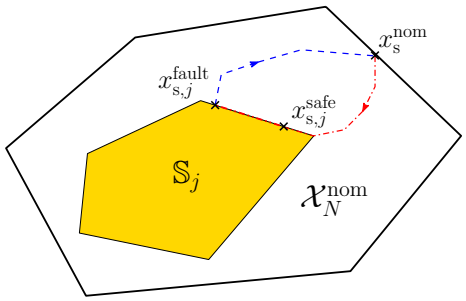

Fig. 1. Schematic illustration of the proposed proactive FTMPC scheme.

To steer the system state x_k inside a *safe*, controllable set within the estimated time t_{f} of failure of actuator j, we apply an exact penalty-function formulation [9]. Let

$$\mathbb{S}_j = \{x \mid G_j x \leq f_j\} \tag{5}$$

be a polyhedral safety set with actuator j rendered inactive, defined by $G_j \in \mathbb{R}^{p \times n}$and $\text{f}_j \in \mathbb{R}^p$. This set can either be defined by operators of the plant or system, in terms of known, conservative safety constraints on the state or a set of controlled variables, or it may be set as the maximum controlled invariant set with actuator j inactive. We apply this latter definition of $\mathbb{S}_j$. Methods to compute controlled invariant sets for LTI systems can be found in for instance [10].

Remark 1. For simplicity, we consider only the fault scenario where the control actuator is rendered entirely inactive at time t_{f}. The scheme can, however, readily be extended to fault scenarios where the actuator loses a fraction of its maximum actuation, by incorporating this in the definition and computation of the safety set $\mathbb{S}_j$.

The set $\mathbb{S}_j$ may often be a strict subset of $\mathcal{X}_N^{\text{nom}}$, and thereby possibly render (2) infeasible when operating at steady state $x_{\text{s}}^{\text{nom}}$ if imposed directly as constraints for all $k \in \mathbb{I}_{[0,N-1]}$ in $P^{\text{nom}}(x)$ at time t_{fw}. Consequently, we must impose the constraints (5) through soft constraints and a penalty

function. To this end, we introduce time-varying, nonnegative vectors $\varepsilon_k \in \mathbb{R}^p$ of slack variables for the polyhedral safety set (5), together with an ℓ_1 penalty norm and soft constraints. At time t_{fw} when the EMPC controller receives warning about an incipient fault in actuator j, we then apply a switching rule to switch from the nominal EMPC problem $P^{\text{nom}}(x)$ to the safe-transition problem $P^{\text{safe}}(x)$ defined by

$$V_N^{\text{safe}}(x) = \min \sum_{k=0}^{N-1} \left(l(x_k,u_k) + \mu \sum_{i=1}^{p} \varepsilon_{ik} \right) \tag{6a}$$

$$\text{s.t.} \quad x_{k+1} = Ax_k + Bu_k, \qquad k \in \mathbb{I}_{[0,N-1]} \tag{6b}$$

$$x_0 = x, \tag{6c}$$

$$(x_k,u_k) \in \mathbb{Z}^{\text{nom}}, \qquad k \in \mathbb{I}_{[0,N-1]} \tag{6d}$$

$$G_j x_k \le f_j + \varepsilon_k, \qquad k \in \mathbb{I}_{[0,N-1]} \tag{6e}$$

$$\varepsilon_k \ge 0, \qquad k \in \mathbb{I}_{[0,N-1]} \tag{6f}$$

$$\varepsilon_{k+1} \le \varepsilon_k, \qquad k \in \mathbb{I}_{[0,N-1]} \tag{6g}$$

$$x_N = x_{\text{s},j}^{\text{safe}}. \tag{6h}$$

In (6), $\mu \ge 0$ is a penalty parameter for the ℓ_1 penalty norm. The new steady-state point $x_{\text{s},j}^{\text{safe}}$ must satisfy $x_{\text{s},j}^{\text{safe}} \in \mathbb{S}_j$, and is obtained by solving the constrained steady-state problem

$$\min\{ l(x,u) \mid x = Ax + Bu,\ (x,u) \in \mathbb{Z}^{\text{nom}} \cap \mathbb{S}_j \}. \tag{7}$$

Assuming (7) is feasible, we denote its optimal objective value $l(x_{\text{s},j}^{\text{safe}}, u_{\text{s},j}^{\text{safe}})$. Solving $P^{\text{safe}}(x)$ on a receding horizon defines an implicit feedback control law $u_{\text{e}}^{\text{safe}}(x) := u_0^*$, similarly as described for $P^{\text{nom}}(x)$ above.

The soft-constraint formulation (6) is equivalent with optimizing the nonsmooth penalty function $\min \sum_{k=0}^{N-1} l(x_k,u_k) + \mu \sum ||\max(0, c_{\mathcal{I}}(x))||_1$ subject to the remaining constraints in (6), where $c_{\mathcal{I}}(x)$ is a vector-function representation of the constraints $G_j x_k - f_j \le 0$ in (5) for all $k \in \mathbb{I}_{[0,N-1]}$. A penalty function $F(x,\mu)$ is termed *exact* if, for a parameter choice $\mu > \bar{\mu}$, where $\bar{\mu}$ is a nonnegative threshold value, the local minimizer of an unconstrained problem $\min_x F(x,\mu)$ is either a KKT point of the original constrained problem, or an infeasible stationary point [9]. For reformulated penalty functions with slack variables and soft constraints where the hard-constrained problem is convex, then exactness of the penalty function implies that the soft and hard constrained problem only differs if the hard-constrained problem is infeasible.

Proposition 1. If Assumption 1 and 2 hold, and $\mu > \bar{\mu}$, where $\bar{\mu}$ is a lower threshold value to ensure that the ℓ_1 penalty function is exact, then the solution $(\mathbf{x}^*, \mathbf{u}^*, \varepsilon^*)$ to the reformulated ℓ_1 penalty function in $P^{\text{safe}}(x)$ will yield an input sequence $\mathbf{u}^*$ that steers the state x_k inside $\mathbb{S}_j$ in minimum number of timesteps.

Proof. With a sufficiently large penalty parameter $\mu > \bar{\mu}$, if $(\mathbf{x}^*, \mathbf{u}^*, 0)$ is infeasible for (6), then exactness of the penalty function (6a) and convexity of problem $P^{\text{safe}}(x)$ ensure constraint satisfaction for those constraints in (6e) that can be satisfied. Consequently, the ℓ_1 exact penalty function yields a solution $(\mathbf{x}^*, \mathbf{u}^*, \varepsilon^*)$ with $\varepsilon_k^* > 0$ only for the first $\bar{k} \in \mathbb{I}_{[0,N-1]}$ (due to (6g)) that would otherwise cause infeasibility if the corresponding hard constraints $G_j x_k \le f_j, \forall k \in \mathbb{I}_{[0,N-1]}$ were enforced, and thereby ensuring that these constraints are violated only if necessary to provide feasibility for $P^{\text{safe}}(x)$. It hence follows that exactness of (6a) ensures an optimal input sequence $\mathbf{u}^*$ such that the constraints $G_j x_k \le f_j$ are violated in minimum number of timesteps, and therefore steers x_k inside $\mathbb{S}_j$ in minimum time. □

Conditions for exactness of the penalty function and a technique for computing μ is provided in Section II-A. For the proposed proactive FTMPC approach, we distinguish between two scenarios relating the estimated fault time t_{f} to the prediction horizon N: If $t_{\text{f}} > t_{\text{fw}} + N$, then feasibility of $P^{\text{safe}}(x)$ at time t_{fw} will ensure $x_k \in \mathbb{S}_j$ within t_{f}. Else, if $t_{\text{f}} \le t_{\text{fw}} + N$, we must include a check of ε^* from the solution of $P^{\text{safe}}(x)$ at time t_{fw}. Let $\varepsilon^*_{t_{\text{f}}|t_{\text{fw}}}$ denote the value of slack vector ε_k^* at prediction time $k = t_{\text{f}} - t_{\text{fw}}$ computed at sampling time t_{fw}. If $\varepsilon^*_{t_{\text{f}}|t_{\text{fw}}} > 0$ and $\mu > \bar{\mu}$, then following Proposition 1, the state cannot reach the set $\mathbb{S}_j$ within the estimated time t_{f} of actuator fault. In this case, the system must be shut down or switched to some emergency mode. Otherwise, $\varepsilon^*_{t_{\text{f}}|t_{\text{fw}}} = 0$, and the state is steered inside $\mathbb{S}_j$ within the estimated fault time t_{f}.

Remark 2. Enforcing hard constraints $G_j x_k \le f_j$ for $k \ge t_{\text{f}} - t_{\text{fw}}$ would not change the solution $(\mathbf{x}^*, \mathbf{u}^*, \varepsilon^*)$ to $P^{\text{safe}}(x)$ when the penalty function is exact. If $\varepsilon_k^* = 0, \forall k \ge t_{\text{f}} - t_{\text{fw}}$ is a feasible solution to $P^{\text{safe}}(x)$, then exactness of the penalty function will ensure this indeed is the solution to $P^{\text{safe}}(x)$. Furthermore, if the required time to steer the state inside $\mathbb{S}_j$ is much less than the estimated time window $t_{\text{f}} - t_{\text{fw}}$, one could consider delaying the transition to the safety set. This approach is, however, generally less robust.

Provided that the EMPC controller with $P^{\text{safe}}(x)$ is able to steer the system inside $\mathbb{S}_j$ within t_{f}, the controller will subsequently steer the system to $x_{\text{s},j}^{\text{safe}}$ as illustrated in Fig. 1, where economic optimal operation inside this safety set can be continued until the fault occurs. We will assume that a separate FDI unit features separate techniques for indicating and distinguishing incipient and actual faults, and as such alerts the EMPC controller if or when the actuator *actually* fails, or is taken out of operation to be replaced. At time instant t_{f} when the fault occurs or the actuator is set inactive, the LTI model and input constraints must be updated to account for the loss of actuation. At this time, the EMPC controller switches to the optimization problem $P^{\text{fault}}(x)$, defined by the convex problem:

$$V_N^{\text{fault}}(x) = \min \sum_{k=0}^{N-1} l(x_k,u_k) \tag{8a}$$

$$\text{s.t.} \quad x_{k+1} = Ax_k + B_j u_k, \qquad k \in \mathbb{I}_{[0,N-1]} \tag{8b}$$

$$x_0 = x, \tag{8c}$$

$$(x_k,u_k) \in \mathbb{Z}_j, \qquad k \in \mathbb{I}_{[0,N-1]} \tag{8d}$$

$$G_j x_k \le f_j, \qquad k \in \mathbb{I}_{[0,N-1]} \tag{8e}$$

$$x_N = x_{\text{s},j}^{\text{fault}}. \tag{8f}$$

The set $\mathbb{Z}_j$ contains updated input constraints, and the new optimal steady-state point, $x_{\mathrm{s},j}^{\mathrm{fault}}$, is computed from

$$\min\{l(x,u) \mid x = Ax + B_j u,\ (x,u) \in \mathbb{Z}_j \cap \mathbb{S}_j\}, \qquad (9)$$

with optimal objective value $l(x_{\mathrm{s},j}^{\mathrm{fault}}, u_{\mathrm{s},j}^{\mathrm{fault}})$. Observe that $x_{\mathrm{s},j}^{\mathrm{fault}} \neq x_{\mathrm{s},j}^{\mathrm{safe}}$ only if the input from the faulty actuator is nonzero at the steady state $(x_{\mathrm{s},j}^{\mathrm{safe}}, u_{\mathrm{s},j}^{\mathrm{safe}})$. We denote $u_{\mathrm{e}}^{\mathrm{fault}}(x) := u_0^*$ as the implicit feedback law obtained by solving $P^{\mathrm{fault}}(x)$ on a receding horizon, where u_0^* is the first element from the solution $\mathbf{u}^*$ to $P^{\mathrm{fault}}(x)$. The EMPC controller operates the system in this fault-updated safe mode until the faulty actuator has been replaced or inspected, in which nominal economic operations of the system is resumed by again switching to solving $P^{\mathrm{nom}}(x)$.

A. Computing the penalty parameter

A critical criteria for the proposed FTMPC scheme is that the system enters the safety set $\mathbb{S}_j$ before the fault occurs. To this end, following Proposition 1, we rely on assuring exactness of the ℓ_1 penalty function (6) to obtain a minimum-time transition to this safety set. Selecting a numerical value for μ may, however, be difficult. It is generally undesirable to assign an arbitrary high value to μ to ensure exactness of the penalty function, as this may lead to violent control action, possibly harmful to the actuators [11], as well as numerical ill-conditioning. We therefore seek to find a lower bound on μ in order to guarantee that the penalty function is exact.

A well-known result for the ℓ_1 penalty functions of an NLP to be exact is that the penalty parameter μ needs to be larger than the absolute value of the largest Lagrangian multiplier for the hard constrained problem, i.e. $\mu > \bar{\mu} = \max \|\lambda^*\|_\infty$ [12, Th. 14.3.1]. Consequently, to compute $\bar{\mu}$ for (6a), the maximum value of the ℓ_∞ norm of the Lagrangian multipliers for the hard-constrained problem for all initial states $x \in \mathbb{S}_j$ must be calculated. To perform this computation, we use the mixed-integer linear programming (MILP) approach developed by [11]. Note that this computation must be performed for each safety set $\mathbb{S}_j$, corresponding to isolated actuators faults as well faults in several actuators simultaneously. However, the computation is done offline. Furthermore, observe that in these computations, we only need to consider the Lagrangian multipliers λ for the soft constraints in (6) [13].

III. Stability Analysis

Nominal stability of EMPC has been proved for systems with a terminal equality constraint, satisfying strong duality [5] or strict dissipativity [4], or with a terminal cost and set for systems satisfying strict dissipativity [3]. In this paper, we base the stability proof on the approach in [5], and make the following assumption.

Assumption 3. If $l(x,u)$ contains other than linear terms, these must be strictly convex, and a constraint qualification, e.g. Slater's condition, must additionally be satisfied at the optimal steady-state point.

If $l(x,u)$ is a linear, economic objective function, the EMPC problems (2), (6) and (8) resort to linear programs (LPs), in which strong duality holds. If $l(x,u)$ is quadratic, e.g. $u_k^T R u_k$, then R must be positive definite, in which the additional assumption of a constraint qualification assures strong duality to hold at optimal steady state. To analyze the stability properties of the proposed FTMPC scheme, we introduce "rotated" stage costs [5],

$$L^{\mathrm{nom}}(x,u) = l(x,u) + (x - Ax - Bu)'\lambda_{\mathrm{s}}^{\mathrm{nom}} - l(x_{\mathrm{s}}^{\mathrm{nom}}, u_{\mathrm{s}}^{\mathrm{nom}}), \qquad (10a)$$

$$L^{\mathrm{safe}}(x,u,\varepsilon) = l^{\mathrm{safe}}(x,u,\varepsilon) + (x - Ax - Bu)'\lambda_{\mathrm{s},j}^{\mathrm{safe}} - l(x_{\mathrm{s},j}^{\mathrm{safe}}, u_{\mathrm{s},j}^{\mathrm{safe}}), \qquad (10b)$$

$$L^{\mathrm{fault}}(x,u) = l(x,u) + (x - Ax - B_j u)'\lambda_{\mathrm{s},j}^{\mathrm{fault}} - l(x_{\mathrm{s},j}^{\mathrm{fault}}, u_{\mathrm{s},j}^{\mathrm{fault}}), \qquad (10c)$$

where $l^{\mathrm{safe}}(x,u,\varepsilon) := l(x_k,u_k) + \mu \sum_{i=1}^{p} \varepsilon_{ik}$ is the point-wise in time stage cost (6a). Moreover, $\lambda_{\mathrm{s}}^{\mathrm{nom}}, \lambda_{\mathrm{s},j}^{\mathrm{safe}}$ and $\lambda_{\mathrm{s},j}^{\mathrm{fault}}$ are Lagrangian multipliers for the LTI steady-state model such that strong duality holds for the three steady-state problems (4), (7) and (9), respectively. Note that strong duality holds by Assumption 3, and that by requiring the steady-state solution $x_{\mathrm{s},j}^{\mathrm{safe}}$ in (7) to be inside in $\mathbb{S}_j$, the steady-state objective value $l(x_{\mathrm{s},j}^{\mathrm{safe}}, u_{\mathrm{s},j}^{\mathrm{safe}})$ in (10b) is independent of ε.

Lemma 1. The following relates the rotated costs (10) and the respective EMPC problems:

1) Solving $P^{\mathrm{nom}}(x)$ in (2) with objective (2a) replaced with $\tilde{V}_N^{\mathrm{nom}}(x) = \min \sum_{k=0}^{N-1} L^{\mathrm{nom}}(x_k,u_k)$ gives equal solutions.
2) Solving $P^{\mathrm{safe}}(x)$ in (6) with the objective (6a) replaced with $\tilde{V}_N^{\mathrm{safe}}(x) = \min \sum_{k=0}^{N-1} L^{\mathrm{safe}}(x_k,u_k,\varepsilon_k)$ gives equal solutions.
3) Solving $P^{\mathrm{fault}}(x)$ in (8) with the objective (8a) replaced with $\tilde{V}_N^{\mathrm{fault}}(x) = \min \sum_{k=0}^{N-1} L^{\mathrm{fault}}(x_k,u_k)$ gives equal solutions.

Proof. All the three rotated costs are point-wise in time summed from $k = 0$ to $N-1$, and the respective EMPC optimization problems all contain a terminal equality constraint. The results hence follow immediately from Lemma 2 in [5]. □

The above lemma is used directly to prove *nominal* stability (perfect model, no disturbances) of the three EMPC modes constituting the proposed proactive FTMPC scheme.

Theorem 1. *(Nominal stability)*: If Assumption 1–3 hold, and $\mu > \bar{\mu}$ such that the ℓ_1 penalty function in (6) is exact, then the following stability properties hold:

1) *(Nominal economic operations)*: $x_{\mathrm{s}}^{\mathrm{nom}}$ is an asymptotically stable steady-state point of the closed-loop system $x_{k+1} = Ax_k + Bu_{\mathrm{e}}^{\mathrm{nom}}(x)$ with Lyapunov function $\tilde{V}_N^{\mathrm{nom}}(x)$ and region of attraction $\mathcal{X}_N^{\mathrm{nom}}$.
2) *(Safety-mode transition)*: At time t_{fw}, if (a) $t_{\mathrm{fw}} + N \leq t_{\mathrm{f}}$ and $\varepsilon_{t_{\mathrm{f}}|t_{\mathrm{fw}}} = 0$, or (b) if $t_{\mathrm{f}} > t_{\mathrm{fw}} + N$, the system will be steered inside the safety set within t_{f}, in which $x_{\mathrm{s},j}^{\mathrm{safe}}$ is an asymptotically stable steady-state point of the closed-loop system $x_{k+1} = Ax_k + Bu_{\mathrm{e}}^{\mathrm{safe}}(x)$ with

Lyapunov function $\tilde{V}_N^{\text{safe}}(x)$ and region of attraction $\mathcal{X}_N^{\text{nom}}$.

3) *(Fault operations)*: $x_{\text{s},j}^{\text{fault}}$ is an asymptotically stable steady-state point of the closed-loop system $x_{k+1} = Ax_k + B_j u_{\text{e}}^{\text{fault}}(x)$ with Lyapunov function $\tilde{V}_N^{\text{fault}}(x)$ and region of attraction $\mathbb{S}_j$

Proof. A sketch of the proof is given for the three parts individually.

Part 1): Recursive feasibility of $P^{\text{nom}}(x)$ is ensured by the terminal equality constraint $x_N = x_{\text{s}}^{\text{nom}}$ and Assumption 2. Furthermore, Assumption 3 ensures strong duality to hold at steady state $x_{\text{s}}^{\text{nom}}$. It can hence be verified that $\tilde{V}_N^{\text{nom}}(x)$ satisfies the properties of a Lyapunov function [5, Th. 1], and in particular that

$$\tilde{V}_N^{\text{nom}}(Ax + Bu_{\text{e}}^{\text{nom}}(x)) \leq \tilde{V}_N^{\text{nom}}(x) - L^{\text{nom}}(x, u_{\text{e}}^{\text{nom}}(x)) \quad (11a)$$
$$\leq \tilde{V}_N^{\text{nom}}(x) - \beta(|x - x_{\text{s}}^{\text{nom}}|)) \quad (11b)$$

for all $x \in \mathcal{X}_N^{\text{nom}}$, and for a K_∞-function $\beta(\cdot)$. This proves part 1) of the theorem.

Part 2): Let $0 < \bar{k} \leq t_{\text{f}} - t_{\text{fw}}$ be an integer, such that $\varepsilon^*_{k|t_{\text{fw}}} = 0$ for all $k \geq \bar{k}$. At sampling time t_{fw}, let $\{\varepsilon_{0|t_{\text{fw}}}, \varepsilon_{1|t_{\text{fw}}}, \ldots, \varepsilon_{\bar{k}-1|t_{\text{fw}}}, 0, \ldots, 0\}$ be a feasible sequence of slack variables, and let $\mathbf{u}$ a feasible control sequence. By applying the feedback control law $u_{\text{e}}^{\text{safe}}(x)$ at time t_{fw}, then at time $t_{\text{fw}} + 1$, the sequence $\{\varepsilon_{1|t_{\text{fw}}}, \ldots, \varepsilon_{\bar{k}-1|t_{\text{fw}}}, 0, 0, \ldots, 0\}$ and $\{u_1, u_2, \ldots, u_{N-1}, u_{\text{s},j}^{\text{safe}}\}$ will be feasible with $(Ax + Bu_{\text{e}}^{\text{safe}}(x))$ as initial condition. This follows from the terminal equality constraint (6h) and by requiring zero slack on the constraints $G_j x \leq f_j$ at the end of the horizon. Feasibility of $P^{\text{safe}}(x)$ for all sample times $t \geq t_{\text{fw}}$ and for all initial states $x \in \mathcal{X}_N^{\text{nom}}$ follows by induction.

For the two scenarios of t_{f} relative to N, the following holds; (a) If $t_{\text{fw}} + N \leq t_{\text{f}}$ and $\varepsilon^*_{t_{\text{f}}|t_{\text{fw}}} = 0$, then by the recursive feasibility, exactness of the penalty term, and Proposition 1, the number of positive slack vectors will decrease by one for each receding horizon iteration, decreasing the total magnitude of the ℓ_1 penalty term. Hence if $\varepsilon^*_{t_{\text{f}}|t_{\text{fw}}} = 0$, then x_k will be steered $\mathbb{S}_j$ within t_{f}, and indeed $x \in \mathbb{S}_j$ for all sampling times $t \geq t_{\text{f}}$ due to the invariance of $\mathbb{S}_j$. If $t_{\text{f}} > t_{\text{fw}} + N$, then it follows immediately that $x_k \in \mathbb{S}_j$ within time t_{f} by feasibility of $P^{\text{safe}}(x)$ at sampling time t_{fw}, and by the same arguments as above. Asymptotic stability of $x_{\text{s},j}^{\text{safe}}$ from switching to $P^{\text{safe}}(x)$ at time t_{fw} can then be established by using $\tilde{V}_N^{\text{safe}}(x)$ for all $x \in \mathcal{X}_N^{\text{nom}}$, and establishing an inequality similar to (11) with $L^{\text{safe}}(x_k, u_k, \varepsilon_k)$ and a K_∞-function $\tilde{\beta}(\cdot)$.

Part 3): If EMPC controller $P^{\text{safe}}(x)$ with control law $u_{\text{e}}^{\text{safe}}(x)$ is able to steer the system state x_k inside $\mathbb{S}_j$ within time t_{f}, then for all initial states $x \in \mathbb{S}_j$, using the same arguments as in part 1) and in [5, Th. 1], it holds that $x_{\text{s},j}^{\text{fault}}$ is an asymptotically stable steady-state point of the closed-loop system $x_{k+1} = Ax_k + B_j u_{\text{e}}^{\text{fault}}(x)$ with region of attraction $\mathbb{S}_j$. □

We comment that asymptotic stability of $P^{\text{safe}}(x)$ may also be achieved by imposing a terminal set and terminal cost rather than a terminal equality constraint, see [3].

IV. NUMERICAL EXAMPLE

In this section, we illustrate the proposed FTMPC scheme with a two-dimensional example. The controlled invariant set $\mathbb{S}_j$ in (5) is computed using the toolbox from [14]. All simulations are performed in YALMIP [15], while CPLEX is used to solve the MILP to compute $\bar{\mu}$ by the approach in [11], and hence define μ. The LTI system is open-loop unstable with matrices

$$A = \begin{bmatrix} 1.3337 & 0.9443 \\ 0.5902 & 1.3337 \end{bmatrix}, \; B = \begin{bmatrix} -0.2572 & -0.3817 \\ -0.2665 & -0.1954 \end{bmatrix}, \quad (12)$$

and economic stage cost $l(x_k, u_k) = -q'x_k + r'u_k$, where $q' = \begin{bmatrix} 10 & 10 \end{bmatrix}$ and $r' = \begin{bmatrix} 3 & 1 \end{bmatrix}$, and with $N = 10$. The constraints on x and u are

$$\begin{bmatrix} 0 \\ 0 \end{bmatrix} \leq \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \leq \begin{bmatrix} 6 \\ 6 \end{bmatrix}, \; \begin{bmatrix} 0 \\ 0 \end{bmatrix} \leq \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} \leq \begin{bmatrix} 5 \\ 15 \end{bmatrix}. \quad (13)$$

We consider the following fault scenario: The EMPC controller receives a warning about an incipient fault in actuator $j = 2$ at sampling time $t_{\text{fw}} = 20$, in which $P^{\text{safe}}(x)$ is invoked. At time $t_{\text{f}} = 40$ the fault hits the system and u_2 is rendered unusable, at which time the EMPC controller switches to solving $P^{\text{fault}}(x)$. Finally, at $t_{\text{fix}} = 60$, the fault is repaired, and the EMPC controller resumes nominal operations by switching to $P^{\text{nom}}(x)$. From the computation of $\bar{\mu} = \max_{x \in \mathbb{S}_2} \|\lambda^*\|_\infty$, cf. Section II-A, we set $\mu = 20$.

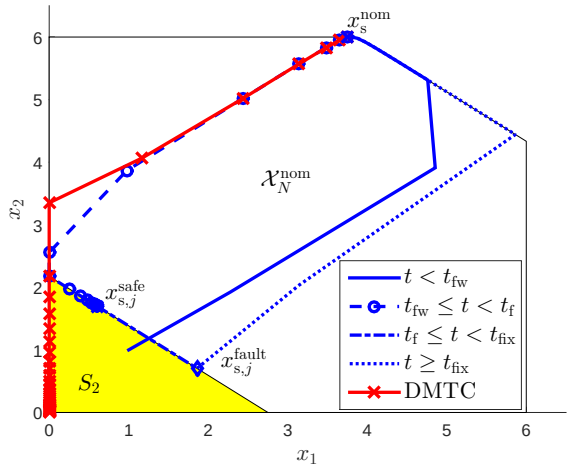

Fig. 2. State-trajectory with the proposed FTMPC scheme applied to the system in (12)–(13). The outer area represents the feasible set $\mathcal{X}_N^{\text{nom}}$ while the yellow triangle represents the safety $\mathbb{S}_2$. The red line shows the state trajectory for an open-loop, discrete minimum-time control (DMTC) solution to reach $\mathbb{S}_2$ from $x_{\text{s}}^{\text{nom}}$, computed by (14) in the Appendix.

Fig. 2 shows the system trajectory, while Fig. 3 shows the input and state time series from applying the proposed FTMPC scheme to the system (12)–(13). The yellow triangle depicts the controlled invariant safety set $\mathbb{S}_2$ for $u_2 = 0$. The system operates at the economic optimal steady-state $x_{\text{s}}^{\text{nom}} = (6.00, 3.75)$ until the controller receives a warning about the incipient fault in actuator u_2. It is evident that a reactive approach which keeps the system operating at $x_{\text{s}}^{\text{nom}}$ until a fault renders u_2 useless, will in this case

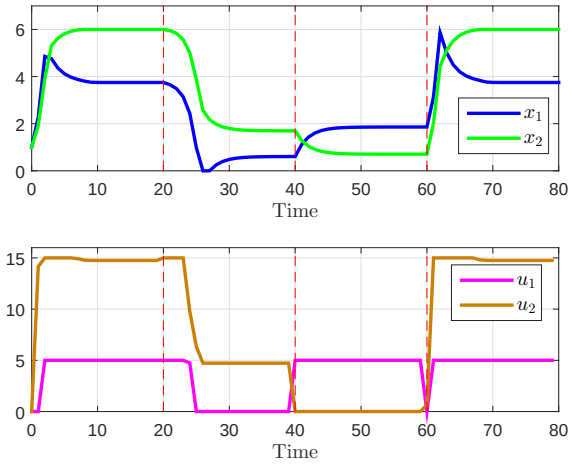

Fig. 3. Closed-loop response of the states and inputs. The warning about an incipient fault is given at sample time $t_{\text{fw}} = 20$, the fault occurs at time $t_{\text{f}} = 40$, and is repaired by time $t_{\text{fix}} = 60$.

make $P^{\text{nom}}(x)$ infeasible and thus destabilize the system. In contrast, the proposed proactive scheme steers the state inside $\mathbb{S}_2$ upon switching from solving $P^{\text{nom}}(x)$ to $P^{\text{safe}}(x)$, and subsequently reaches the temporary steady-state point $x_{\text{s},j}^{\text{safe}} = (0.60, 1.69)$. Observe that the state enters $\mathbb{S}_2$ at a different point than the steady state $x_{\text{s},j}^{\text{safe}}$ in order to minimize the number of timesteps with nonzero slack variables. When the fault occurs, the EMPC controller switches to solving $P^{\text{fault}}(x)$, the faulty model is updated, and the system is steered to the new economically optimal steady-state point $x_{\text{s},j}^{\text{fault}} = (1.86, 0.71)$. At time t_{fix}, actuator u_2 is repaired, nominal operation is resumed by switching back to solving $P^{\text{nom}}(x)$, and the system is steered back to $x_{\text{s}}^{\text{nom}}$. Observe from Fig. 3 that there are no discontinuities in the states at the times of switching between the EMPC modes.

In Fig. 2, we compare our proposed FTMPC scheme with the solution to the open-loop, discrete minimum-time control (DMTC) problem (14) in the Appendix, which gives the control input required to reach the set $\mathbb{S}_2$ from $x_{\text{s}}^{\text{nom}}$ in minimum time. The two approaches both require eight timesteps to reach $\mathbb{S}_2$, demonstrating as such that the exact-penalty formulation yields a time-optimal transition to $\mathbb{S}_2$, while it can seen that the solution to minimum-time problem (14) gives a different state trajectory. This follows from the well-known property that discrete minimum-time control is in general nonunique [16], and does not necessarily give a control input that is bang-bang.

V. Concluding remarks

The proactive FTMPC scheme proposed in this paper ensures a minimum-time escape to a safety set, and thereby, provided the set can be reached within the estimated fault time, circumvents the infeasibility issues that may be encountered in reactive FTMPC approaches for actuator faults. The approach allows continued economic operation of the system during the subsequent actuator repair, and may thus be a constructive and cost-saving supplement for handling incipient actuator faults as a part of efficient fault-tolerant MPC schemes.

References

[1] D. Q. Mayne, "Model predictive control: Recent developments and future promise," *Automatica*, vol. 50, no. 12, pp. 2967–2986, 2014.

[2] J. M. Maciejowski, "Modelling and predictive control: Enabling technologies for reconfiguration," *Annu. Rev. Control*, vol. 23, pp. 13–23, 1999.

[3] R. Amrit, J. B. Rawlings, and D. Angeli, "Economic optimization using model predictive control with a terminal cost," *Annu. Rev. Control*, vol. 35, no. 2, pp. 178–186, 2011.

[4] D. Angeli, R. Amrit, and J. B. Rawlings, "On average performance and stability of economic model predictive control," *IEEE Trans. Autom. Control*, vol. 57, no. 7, pp. 1615–1626, 2012.

[5] M. Diehl, R. Amrit, and J. B. Rawlings, "A Lyapunov function for economic optimizing model predictive control," *IEEE Trans. Autom. Control*, vol. 56, no. 3, pp. 703–707, 2011.

[6] L. Lao, M. Ellis, and P. D. Christofides, "Proactive fault-tolerant model predictive control," *AIChE J.*, vol. 59, no. 8, 2013.

[7] F. Salfner and M. Malek, "Using hidden semi-Markov models for effective online failure prediction," in *Proc. of the IEEE Symp. on Reliable Distributed Systems*, 2007, pp. 161–174.

[8] T. I. Bø and T. A. Johansen, "Dynamic Safety Constraints by Scenario Based Economic Model Predictive Control," in *Proc. IFAC World Congress*, 2014, pp. 9412–9418.

[9] T. Pietrzykowski, "An exact potential method for constrained maxima," *SIAM J. Numer. Anal.*, vol. 19, no. 2, pp. 786–789, 1969.

[10] E. Kerrigan and J. Maciejowski, "Invariant sets for constrained nonlinear discrete-time systems with application to feasibility in model predictive control," in *Conf. Decision Control*, 2000, pp. 4951–4956.

[11] M. Hovd and F. Stoican, "On the design of exact penalty functions for MPC using mixed integer programming," *Comput. Chem. Eng.*, vol. 70, no. 5, pp. 104–113, 2014.

[12] R. Fletcher, *Practical Methods of Optimization*, 2nd ed. Wiley, 1987.

[13] S. Janesch and L. Santos, "Exact penalty methods with constrained subproblems," *Investigacióon Operativa*, vol. 7, pp. 55–65, 1997.

[14] E. Kerrigan, "Matlab invariant set toolbox," 2005. [Online]. Available: http://www-control.eng.cam.ac.uk/eck21/matlab/invsetbox/index.html

[15] J. Løfberg, "YALMIP : A toolbox for modeling and optimization in MATLAB," in *Proc.of the CACSD Conference*, Taipei, Taiwan, 2004.

[16] S. Keerthi and E. Gilbert, "Computation of minimum-time feedback control laws for discrete-time systems with state-control constraints," *IEEE Trans. Autom. Control*, vol. 32, no. 5, pp. 432–435, 1987.

Appendix

The minimum time required to steer a linear system from an initial given feasible state x_0, inside a compact set $\mathbb{S} = \{x \mid Gx \leq f\}$, with the initial state $x_0 \notin \mathbb{S}$, can be computed by the following MILP:

$$\min \sum_{k=1}^{N} -w_k y_k \tag{14a}$$

$$\text{s.t.} \quad x_{k+1} = Ax_k + Bu_k, \qquad k \in \mathbb{I}_{[0,N-1]} \tag{14b}$$

$$x_0 = \text{given}, \tag{14c}$$

$$(x_k, u_k) \in \mathbb{Z}^{\text{nom}}, \qquad k \in \mathbb{I}_{[0,N]} \tag{14d}$$

$$Gx_k \leq f + M(1 - y_k), \qquad k \in \mathbb{I}_{[1,N]} \tag{14e}$$

$$y_k = \{0, 1\}, \qquad k \in \mathbb{I}_{[1,N]} \tag{14f}$$

In (14), w_k is a sequence of positive, strictly increasing weights, e.g. $w_k := k$, and M is a big-M parameter. If (14) has a feasible integer solution with $y_k = 1$ for some k, the minimum time $t^{\min}$ to get the state x_k inside the set $\mathbb{S}$ is given by the integer $k^{\min}$ for which the binary y_k first takes the value 1, i.e. $t^{\min} = \{k^{\min} | y_k = 1,\ \forall k \geq k^{\min}\}$. Observe that the negativity in (14a) ensures that the system stays in $\mathbb{S}$ for all positive times when first inside.