

Tracking Limitations and Rate-Consistent Safety Filtering for Constrained Mechanical Systems

Mehdi Heydari Shahna

`mehdi.heydarishahna@tuni.fi`

Tampere University <https://orcid.org/0000-0002-1310-5392>

Jouni Mattila

Tampere University <https://orcid.org/0000-0003-1799-4323>

Research Article

Keywords: Control barrier functions, virtual decomposition control, RoboCompiler, passivity-based control

Posted Date: October 16th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-11381118/v1>

License:   This work is licensed under a Creative Commons Attribution 4.0 International License.
[Read Full License](#)

Additional Declarations: The authors declare no competing interests.

Tracking Limitations and Rate-Consistent Safety Filtering for Constrained Mechanical Systems

Mehdi Heydari Shahna  and Jouni Mattila 

Abstract—Reference-level and effort-level safety filters can impose incompatible constraint-approach rates in mechanical systems. This paper characterizes the resulting velocity-tracking limitations and develops a rate-consistent control barrier function (CBF) framework. A controller-independent lower bound, expressed through the realized reference slack, quantifies the kinetic tracking error at constraint activation or a preceding comparison time. Repeated activations with uniformly positive preceding slack, bounded comparison intervals and bounded kinetic gradients preclude convergence. For virtual decomposition control (VDC) with inertia-proportional gains and a kinetic effort metric, a projection-based inequality characterizes the effect of safety corrections on tracking dissipation, including dependent binding constraints. An exact constraint identity separates reference-rate mismatch, mechanical curvature and feedforward defects. An acceleration-level reference filter enforces a sufficient rate-consistency condition. Under the stated correction-support and curvature hypotheses, the nominal loop preserves exact initial tracking; a uniformly positive net dissipation rate gives exponential decay and an explicit ultimate error bound under bounded defects. For two-sided coordinate limits with a nonsingular coordinate-limit Jacobian on a compact admissible configuration set and unconstrained efforts, strict feasibility and global continuation are established under nominal actuation. RoboCompiler supplies the shared mechanical interfaces for VDC and both CBF layers. Continuous-time benchmarks illustrate the analytical bounds. In repeated-limit experiments, two sampled hydraulic excavator simulations reduce onset errors by factors 3.3 and 3.6 and positive safety-port energy by more than two orders of magnitude, with comparable minimum clearances.

Index Terms—Control barrier functions, virtual decomposition control, RoboCompiler, passivity-based control.

I. INTRODUCTION

SAFETY filtering for constrained mechanical systems must coordinate admissible motion commands with the actuator efforts that realize them. Control barrier functions (CBFs) provide systematic constraints at both levels [1], [2]. First-order reference filters constrain commanded velocities [3]–[5], whereas effort-level filters enforce second-order conditions on the physical motion [6], [7]. The two layers can therefore impose different approach rates at the same geometric boundary. A reference filter may drive its nonnegative barrier slack to zero in finite time, while the effort layer restricts how quickly the corresponding barrier quantity of the actual motion can decrease. This mismatch can force velocity-tracking error even with ideal actuation and exact nominal feedforward.

This work was supported by the Post Docs in Companies (PoDoCo) program, Finland. Authors are with the Faculty of Engineering and Natural Sciences, Tampere University, Tampere, Finland. (Corresponding author e-mail: mehdi.heydarishahna@tuni.fi).

The source code and mission videos are available at <https://github.com/Mehdi-Heydari-Shahna/RateConsistentCBF>.

Energy-based mechanical tracking provides a direct way to quantify this interaction. The Slotine–Li construction [8] and virtual decomposition control (VDC) [9], [10] use mechanical structure to establish tracking properties. VDC organizes the controller through body-level laws and tracking storage, including subsystem controllers, observers and hydraulic closed-chain mechanisms [11]–[13]. For required and actual velocities u_r and u , let $s = u_r - u$ and $S = \frac{1}{2}s^\top Ms$, where M is the inertia matrix. With exact feedforward, a nominal model and feedback $K = kM$, the unfiltered balance is $\dot{S} = -2kS$. An effort correction Δ contributes the power $P_f = -s^\top C\Delta$, where C maps actuator efforts to generalized forces. We call this contribution the *safety port*. The central problem is to relate this power and the tracking error to the evolution of the required motion’s barrier slack.

Related work. Hierarchical and reduced-order CBF methods connect high-level safety conditions to the dynamics of a tracking loop. Energy-based kinematic control [3], exponential velocity-tracking conditions [4], and reduced-order formulations [14], [15] provide mechanisms for transferring safety between layers. Multirate architectures also coordinate planning and actuation through tracking and timing conditions [16], [17]. Reference governors modify commands to maintain constraint satisfaction [18], [19], while integral CBFs accommodate dynamically defined control laws [20]. CBF backstepping constructs safe controllers through virtual controls [21]. Closely related proxy CBFs generate a virtual reference and combine its safety construction with a Lyapunov-based subsystem that bounds the tracking error [22]. The architecture considered here retains a separate effort-level safety filter and examines its effect on tracking of the reference generated by the first layer.

A complementary literature addresses feasibility and compatibility. Output-box CBF compatibility and the associated degradation of tracking objectives are studied in [23]. Safe Euler–Lagrange control [24] and feasibility conditions under input constraints [25], [26] characterize admissible safety programs. Compatibility between safety and stabilization [27], together with analyses of safety-filter-induced equilibria [28]–[30], describes further ways in which filtering affects performance. Our analysis focuses on the required-velocity slack and its closing rate, connecting that rate to a tracking-error lower bound and to the dissipation of the mechanically structured tracking loop.

The energetic effect of CBF corrections has been characterized for port-Hamiltonian systems [31], [32]. Passive interaction controllers [33] and safety-aware energy tanks [34] also connect constraint enforcement to energy exchange. For

passivity-based manipulator control, [35] optimizes the input of a reference system while constraining its storage derivative. Here, the analyzed storage is the kinetic velocity-error storage. A kinetic effort-projection metric connects the geometry of multiple binding constraints to the dissipation supplied by the nominal tracking law. The exact constraint identity (Lemma 3) then expresses the remaining contribution through reference-rate mismatch, mechanical curvature and feedforward defects.

Objective and contributions. We address three connected questions: when does reference-slack evolution force a tracking limitation; how does the effort correction modify tracking dissipation; and which reference dynamics make the two layers rate consistent? For mechanical systems satisfying $M = N + N^\top$, the paper establishes the following results.

- 1) *A controller-independent tracking limitation* (Theorem 1 and Corollary 1). A lower bound expressed through the realized reference slack quantifies the kinetic tracking error at constraint activation or a preceding comparison time. Repeated activations with uniformly positive preceding slack, bounded comparison intervals and bounded kinetic gradients preclude convergence. A constant-rate, curvature-free approach with a single supporting barrier attains the onset bound (Remark 1).
- 2) *A projection-based dissipation characterization* (Theorems 2 and 3). For the VDC tracking law with $K = kM$ and $CH^{-1}C^\top = M$, projection geometry bounds safety-support power, including dependent binding constraints. The exact constraint identity of Lemma 3 separates reference-rate mismatch, mechanical curvature and feedforward defects, yielding an explicit tracking-storage inequality.
- 3) *A constructive rate-consistency condition* (Propositions 1 and 2, Theorem 4 and Corollary 2). Exact nominal tracking requires each reference slack to satisfy the rate condition associated with its second-order effort barrier. An acceleration-level reference filter enforces a sufficient common rate condition. Under the stated correction-support and curvature hypotheses, the resulting loop preserves exact initial nominal tracking and admits quantitative decay and defect-dependent bounds. For two-sided coordinate limits with a nonsingular coordinate-limit Jacobian on a compact admissible configuration set and unconstrained efforts, Theorem 5 additionally establishes strict feasibility and global continuation under nominal actuation.

The mechanical assumptions and assembled tracking law define the scope of the theory independently of a particular model-generation tool. In the evaluated realization, RoboCompiler generates the mechanical, actuator and barrier interfaces from a common mechanism graph [36]; VDC supplies the body-level tracking laws and assembled storage; and the CBF layers coordinate required motion and admissible efforts (Figs. 1 and 2).

A scalar example and a six-joint Pinocchio model [37] illustrate the analytical lower bounds and tracking estimates. Sampled MuJoCo simulations [38] of two hydraulic excavators, Komatsu and HEAP, assess the implemented framework with closed kinematic chains and force loops; ablations distin-

guish reference-rate consistency from reference smoothing. A conditioning construction relates correction feedback to anti-windup and pseudo-control hedging [39], [40] and identifies its effect on tracking of the original reference (Proposition 4). All proofs appear in the main-paper Appendix.

Section II defines the mechanical setting and safety filters. Sections III and IV establish the tracking limitation and dissipation bounds. Section V develops rate consistency and feasibility, and Section VI treats conditioning. Sections VII and VIII present numerical validation and design implications. Section IX concludes the paper.

Notation. $\langle a, b \rangle_M = a^\top M b$ and $\|a\|_M^2 = a^\top M a$; $\|y\|_{\Lambda^{-1}}^2 = y^\top \Lambda^{-1} y$ for symmetric $\Lambda \succ 0$. For $x \in \mathbb{R}$, $[x]^+ = \max\{x, 0\}$ and $[x]^- = \max\{-x, 0\}$, entrywise for vectors. Unsubscripted vector norms are Euclidean, matrix $\|\cdot\|_2$ is the induced Euclidean norm, and I_d denotes the d -dimensional identity (its subscript is omitted when clear). “A.e.” means almost every t . For a set A of constraints, J_A , Γ_A , w_A , χ_A and $\Pi_A^{(\beta)}$ denote the matrices and vectors restricted to the rows or entries $i \in A$.

II. SETTING AND PROBLEM STATEMENT

A. Mechanical setting and the assembled VDC law

We consider independent coordinates $q \in \mathcal{Q} \subset \mathbb{R}^d$ ($\mathcal{Q}$ open) and speeds $u = \dot{q}$, with closed kinematic chains reduced to these coordinates. The analysis uses the mechanical model and assembled VDC tracking law specified below. In the evaluated realization, RoboCompiler supplies their mechanical, actuator and barrier interfaces from a common mechanism graph [36]. The two CBF layers use these shared interfaces to coordinate the required motion and actuator efforts. The mechanical model is

$$\dot{q} = u, \quad M\dot{u} + Nu + g = Cf + \tau_e. \quad (1)$$

Here $M \in \mathbb{R}^{d \times d}$ is the inertia matrix, $N \in \mathbb{R}^{d \times d}$ contains velocity-coupling terms, $g \in \mathbb{R}^d$ is the gravity and bias force, $f \in \mathbb{R}^m$ contains the delivered actuator efforts, $C \in \mathbb{R}^{d \times m}$ maps these efforts to generalized forces, and $\tau_e \in \mathbb{R}^d$ is the external force.

Assumption 1 (model). $M = M(t, q) = M^\top \succ 0$ is continuously differentiable; $N = N(t, q, u)$, $g = g(t, q, u)$ and $C = C(t, q)$ are continuous; $\text{rank } C = d$; $\tau_e(t)$ is locally bounded and measurable; and along every C^1 curve with $\dot{q} = u$,

$$\frac{d}{dt} M = N + N^\top. \quad (2)$$

For a required velocity $u_r(t)$ and required acceleration $a_r(t)$ (the feedforward), the assembled VDC law computes nominal efforts φ_r through

$$C\varphi_r = Ma_r + Nu_r + g - \hat{\tau}_e + K(u_r - u), \quad (3)$$

where $\hat{\tau}_e$ is a load estimate and $K = K^\top \succ 0$ is the velocity feedback. In the compiled rigid-body realization, let $\mathcal{B}$ index the bodies, $J_B(q) \in \mathbb{R}^{6 \times d}$ be the body-frame spatial-velocity Jacobian of body B , and $M_B \in \mathbb{R}^{6 \times 6}$ and $K_B \in \mathbb{R}^{6 \times 6}$ its spatial inertia and feedback gain in that frame. The required and actual twists are evaluated at the same configuration and

prescribed base motion, so their error is $e_B = J_B s$, with $s := u_r - u$. Virtual-work assembly gives

$$\begin{aligned} M &= \sum_{B \in \mathcal{B}} J_B^\top M_B J_B, & K &= \sum_{B \in \mathcal{B}} J_B^\top K_B J_B, \\ S &:= \frac{1}{2} \|s\|_M^2 = \sum_{B \in \mathcal{B}} \frac{1}{2} e_B^\top M_B e_B. \end{aligned} \quad (4)$$

Thus body gains $K_B = kM_B$ assemble to $K = kM$. These identities connect the VDC body storage to the compiled mechanical model; the analysis below applies to every realization of (3) satisfying Assumption 1. For $m > d$, any selection among the effort solutions is admitted. We write $e_a := \dot{u}_r - a_r$ for the feedforward defect. The commanded efforts are $\varphi = \varphi_r + \Delta$, where Δ is the correction of the effort layer below, and the mismatch $e_m := M^{-1}(C(f - \varphi) + \tau_e - \hat{\tau}_e)$ collects force-loop and load-estimation errors.

Lemma 1 (storage balance). *Under Assumption 1, if u and u_r are locally absolutely continuous and (1), (3) hold a.e., then S is locally absolutely continuous and a.e.*

$$\dot{S} = -s^\top K s + \langle s, e_a - e_m \rangle_M + P_f, \quad P_f := -s^\top C \Delta; \quad (5)$$

for $K = kM$ the first term is $-2kS$.

B. Barrier constraints and the two layers

Let $h_i(t, q)$, $i \in \mathcal{I} = \{1, \dots, R\}$, be barrier functions (clearances, stroke and joint limits), continuously differentiable with locally Lipschitz derivatives, with rates $\alpha_{1,i}, \alpha_{2,i} > 0$ and constant standoffs $\sigma_i \geq 0$. We write $\tilde{h}_i := h_i - \sigma_i$,

$$\dot{h}_i = b_i + J_i u, \quad b_i := \partial_t h_i, \quad J_i := \partial_q h_i, \quad \nu_i := M^{-1} J_i^\top,$$

so that ν_i is the gradient of h_i in the kinetic metric and $J_i v = \langle \nu_i, v \rangle_M$. Along a motion, $t \mapsto b_i(t, q(t))$ and $t \mapsto J_i(t, q(t))$ are locally Lipschitz, and $\dot{b}_i, \dot{J}_i$ denote their derivatives, which exist a.e. The first- and second-order CBF functions of the motion are

$$\tilde{\psi}_{1,i} := \dot{h}_i + \alpha_{1,i} \tilde{h}_i, \quad \tilde{\psi}_{2,i} := \dot{\tilde{\psi}}_{1,i} + \alpha_{2,i} \tilde{\psi}_{1,i}. \quad (6)$$

First layer (baseline: velocity level). Given a nominal velocity $u_n(t, q)$ and the first-order function $\tilde{z}_i(v) := b_i + J_i v + \alpha_{1,i} \tilde{h}_i$ of a velocity v , the required velocity is

$$u_r = \arg \min_{v \in \mathcal{V}} \frac{1}{2} \|v - u_n\|_{Q_v}^2 \quad \text{s.t.} \quad \tilde{z}_i(v) \geq 0 \quad (i \in \mathcal{I}), \quad (7)$$

with a metric $Q_v \in \mathbb{R}^{d \times d}$, $Q_v \succ 0$, and a closed convex set $\mathcal{V} \subset \mathbb{R}^d$ (capability constraints). Along a motion, $\tilde{z}_i(t) := \tilde{z}_i(u_r(t))$ is the *slack* of constraint i : the first-order function that the motion would have if it followed the required velocity. Since $\tilde{\psi}_{1,i} = b_i + J_i u + \alpha_{1,i} \tilde{h}_i$,

$$w_i := J_i s = \tilde{z}_i - \tilde{\psi}_{1,i}. \quad (8)$$

We call constraint i *active* at t if $\tilde{z}_i(t) = 0$, and an *activation* the beginning of an interval on which it is active.

Effort layer (second order). With the model acceleration $\hat{a}(\varphi') := M^{-1}(C\varphi' + \hat{\tau}_e - Nu - g)$ of a command φ' , the model value of the second-order function is

$$\hat{\psi}_{2,i}(\varphi') := J_i \hat{a}(\varphi') + \dot{J}_i u + \dot{b}_i + (\alpha_{1,i} + \alpha_{2,i}) \dot{h}_i + \alpha_{1,i} \alpha_{2,i} \tilde{h}_i, \quad (9)$$

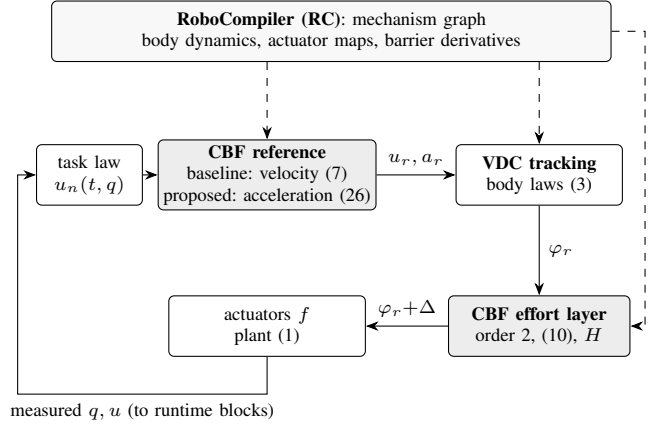


Fig. 1. RC-VDC-CBF architecture. RoboCompiler generates the mechanical and barrier interfaces (dashed arrows). The runtime path combines CBF reference generation, VDC tracking and CBF effort filtering. Both shaded layers use the same barriers; the effort correction exchanges the safety-port power $P_f = -s^\top C \Delta$ with the assembled VDC storage $S = \frac{1}{2} \|s\|_M^2$.

affine in φ' with the row vector $G_i := J_i M^{-1} C$, and the command is

$$\varphi = \arg \min_{\varphi' \in \mathcal{F}} \frac{1}{2} \|\varphi' - \varphi_r\|_H^2, \quad \mathcal{F} := \{\varphi' : \hat{\psi}_{2,i}(\varphi') \geq 0 \forall i\} \cap \Phi, \quad (10)$$

with a metric $H \in \mathbb{R}^{m \times m}$, $H \succ 0$, and a closed convex polyhedral set $\Phi \subset \mathbb{R}^m$ (effort bounds, contact constraints). We write all constraints of $\mathcal{F}$ as $G_j \varphi' \geq r_j$ and say that constraint j *binds* if equality holds at φ . The true second-order function is $\hat{\psi}_{2,i} = \hat{\psi}_{2,i}(\varphi) + J_i e_m$, because $\dot{u} = \hat{a}(\varphi) + e_m$. The loop is shown in Fig. 1.

Assumption 2 (design). (a) $K = kM$, $k > 0$. (b) The effort metric is *kinetic*: $CH^{-1}C^\top = M$. (c) Both layers use the same h_i , $\alpha_{1,i}$ and σ_i .

For $m = d$, condition (b) uniquely gives $H = C^\top M^{-1} C$. For redundant actuation, $H = C^\top M^{-1} C + R_0$ is a sufficient construction when $R_0 \succeq 0$, $R_0 C^\top = 0$, and $H \succ 0$; Lemma 5 gives the general characterization. With barrier constraints only, the command then gives the acceleration nearest to the nominal one in the kinetic norm among those that satisfy the constraints, a form of Gauss' principle of least constraint [41]. With $C^\sharp := H^{-1} C^\top M^{-1}$ and $\hat{s} := C^\sharp M s$, condition (b) gives

$$P_f = -\langle \hat{s}, \Delta \rangle_H, \quad \|\hat{s}\|_H = \|s\|_M, \quad G_i \hat{s} = w_i. \quad (11)$$

C. Solutions and safety

Definition 1 (solution). A *solution* on $I = [0, T)$ consists of $q \in C^1(I; \mathcal{Q})$, locally absolutely continuous u , u_r , and locally bounded measurable $a_r, \varphi_r, \varphi, f, \hat{\tau}_e$, such that a.e. on I : (1) and (3) hold, $\mathcal{F}(t) \neq \emptyset$ and φ is given by (10). It is *nominal* if $e_m = 0$ a.e.

The proposed first layer constructs an absolutely continuous u_r . Strict feasibility gives local existence (Proposition 3); for two-sided limits of all coordinates, feasibility and global continuation follow from the data (Theorem 5). Sections III

and IV apply to every required velocity satisfying Definition 1. Safety follows by the comparison argument for exponential CBF constraints [6], [7], with the mismatch margin of [42]:

Lemma 2 (safety). *For nominal solutions the safe set $\mathcal{C}(t) := \{(q, u) : \tilde{h}_i(t, q) \geq 0, \tilde{\psi}_{1,i}(t, q, u) \geq 0 \ \forall i\}$ is forward invariant (we write $\mathcal{C}$ for short). If $|J_i e_m| \leq \varepsilon_i$ a.e. with a constant $\varepsilon_i \geq 0$, every solution that starts in $\mathcal{C}$ satisfies $h_i \geq \sigma_i - \varepsilon_i/(\alpha_{1,i}\alpha_{2,i})$.*

The standoff supplies the margin $\alpha_{1,i}\alpha_{2,i}\sigma_i$ on the unshifted constraint and keeps $h_i \geq 0$ whenever this margin covers ε_i , independently of the reference generator. All rates $\alpha_{1,i}$, $\alpha_{2,i}$ and k have units s^{-1} ; σ_i has the units of h_i .

D. Running example and problem statement

Example 1 (one degree of freedom). Let $d = 1$, $M = C = H = 1$, $N = g = \tau_e = \hat{\tau}_e = 0$, an ideal effort source ($f = \varphi$), $\mathcal{V} = \mathbb{R}$, $\Phi = \mathbb{R}$, $h = q$ with rates α_1, α_2 , no standoff, and a C^1 nominal velocity $u_n(t)$ of period T_p with mean $-\bar{v} < 0$ and maximum $v^+ > 0$: a task that asks to cross the limit in every period. The first layer (7) is $u_r = \max\{u_n, -\alpha_1 q\}$, the effort layer is $\varphi = \max\{\varphi_r, -(\alpha_1 + \alpha_2)u - \alpha_1\alpha_2 q\}$, and $\tilde{z} = u_r + \alpha_1 q$. The constraint is active where $u_n + \alpha_1 q \leq 0$: there the required velocity has a kink and follows $-\alpha_1 q$. For $u_n = 0.5 \sin(\pi t) - 0.1$ m/s ($T_p = 2$ s) and the rates (6, 16), Fig. 3(b) shows the velocity error of this loop with the law (3) and the exact feedforward $a_r = \dot{u}_r$: it is the same in every period from the third one on, for $k = 12, 30$ and 100 .

This example motivates two problems: characterize the irreducible error of repeated constraint activations, and construct a reference generator that preserves the tracking certificate while the effort layer enforces safety.

III. A LOWER BOUND FOR FIRST-ORDER CONSTRAINTS

The effort layer keeps $\tilde{\psi}_{2,i} \geq 0$, so the first-order function of the actual motion cannot decrease faster than at the rate $\alpha_{2,i}$. The first layer (7) lets the slack of the required motion reach zero at any speed. The difference of the two is a velocity error.

Theorem 1 (lower bound). *Let Assumption 1 hold and consider a nominal solution in the sense of Definition 1 with the requirement (3) dropped: φ_r is any locally bounded measurable nominal effort in (10) and u_r any locally absolutely continuous required velocity. For every barrier constraint i and all $t_a \leq t_2$ in I , $\tilde{\psi}_{1,i}(t_2) \geq e^{-\alpha_{2,i}(t_2-t_a)}\tilde{\psi}_{1,i}(t_a)$, with equality if the effort constraint i binds a.e. on $[t_a, t_2]$. If constraint i is active at t_2 , then, with $\theta := t_2 - t_a$,*

$$-J_i s(t_2) = \tilde{\psi}_{1,i}(t_2) \geq e^{-\alpha_{2,i}\theta}(\tilde{z}_i(t_a) - J_i s(t_a)). \quad (12)$$

Consequently, for every number $\bar{v} > 0$ with $\bar{v} \geq \max\{\|\nu_i(t_a)\|_M, \|\nu_i(t_2)\|_M\}$:

- (i) $\max\{\|s(t_2)\|_M, \|s(t_a)\|_M\} \geq \tilde{z}_i(t_a)/(\bar{v}(e^{\alpha_{2,i}\theta} + 1))$;
- (ii) if the solution exists on $[0, \infty)$, $\|\nu_i\|_M \leq \bar{v}$, and there are times $t_n \rightarrow \infty$ at which constraint i is active and $\theta_n \in [0, \bar{\theta}]$ with $\tilde{z}_i(t_n - \theta_n) \geq z_0 > 0$, then

$$\limsup_{t \rightarrow \infty} \|s(t)\|_M \geq \frac{z_0}{\bar{v}(e^{\alpha_{2,i}\bar{\theta}} + 1)} > 0.$$

Corollary 1 (size of the error at an activation). *Under the hypotheses of Theorem 1, let constraint i be active at t_2 and $t_a := t_2 - 1/\alpha_{2,i} \in I$. Then*

$$|J_i s(t_2)| + e^{-1}|J_i s(t_a)| \geq e^{-1}\tilde{z}_i(t_a). \quad (13)$$

If the slack closes at least at the rate $v > 0$ ($\dot{\tilde{z}}_i \leq -v$ a.e.) on $[t_2 - \bar{\theta}, t_2]$ with $\bar{\theta} \geq 1/\alpha_{2,i}$, then $\tilde{z}_i(t_2 - \theta) \geq v\theta$ for $\theta \in [0, \bar{\theta}]$, in particular $\tilde{z}_i(t_a) \geq v/\alpha_{2,i}$, and $\theta = 1/\alpha_{2,i}$ maximizes the resulting bound $v\theta e^{-\alpha_{2,i}\theta}$ of (12) (without the term $J_i s(t_2 - \theta)$) over $\theta \in [0, \bar{\theta}]$.

The theorem and corollary use only the second-order barrier inequality and the identity (8); their conclusions therefore do not depend on the nominal effort law. The bound concerns tracking of the required velocity u_r and is expressed through its realized slack profile. For a fixed profile satisfying the theorem hypotheses, changing the nominal feedback gain does not remove the bound. A bound determined directly by prescribed problem data additionally requires a corresponding lower bound on the preceding slack, as in Example 1. The general result bounds the maximum error at activation and a preceding comparison time; Remark 1 identifies a case in which the onset bound is attained.

Remark 1 (attainment). Let one barrier constraint support the correction (Φ inactive), let its slack close at the constant rate v until it becomes active at t_2 , without curvature ($\gamma_i = 0$ in Section IV), let the solution be nominal, and let the law (3) with $K = kM$ and exact feedforward track exactly until the effort constraint binds. At $s = 0$ the nominal value of the effort constraint is $\tilde{z}_i + \alpha_{2,i}\tilde{z}_i$ by Lemma 3, so the constraint binds once $\tilde{z}_i = v/\alpha_{2,i}$, i.e. at $t_a = t_2 - 1/\alpha_{2,i}$, and binds until t_2 for every $k > 0$. Then (13) holds with equality, and

$$|J_i s(t_2)| = \tilde{\psi}_{1,i}(t_2) = \frac{v}{e\alpha_{2,i}} : \quad (14)$$

the error along the gradient is fixed by the approach speed and the barrier rate, not by the gain.

Example 1 (continued). For every nominal effort law φ_r and every solution on $[0, \infty)$ that starts in $\mathcal{C}$,

$$\limsup_{t \rightarrow \infty} |s(t)| \geq \min\left\{\bar{v}, \frac{v^+}{e^{\alpha_{2,i}T_p} + 1}\right\} > 0. \quad (15)$$

If the constraint is active at times $t_n \rightarrow \infty$, Theorem 1(ii) applies with $z_0 = v^+$ and $\bar{\theta} = T_p$, because $\tilde{z} = \max\{u_n + \alpha_1 q, 0\} \geq v^+$ wherever $u_n = v^+$. Otherwise $u_r = u_n$ after some time, and $q \geq 0$ forces the mean of $-s$ over long intervals to be at least $\bar{v}$. Solutions exist for every $k > 0$: with $\varphi_r = \dot{u}_n + k(u_r - u)$, i.e. (3) with $a_r = \dot{u}_n$, the closed loop is continuous in t and globally Lipschitz in (q, u) , and u_r is locally Lipschitz along it. The constant in (15) is small, because it only uses that the slack was v^+ one period earlier; it proves non-convergence. Corollary 1 gives the size: in Section VII-A it is attained to within 0.7% wherever the slack closes at a nearly constant rate. Hence the loop with the first layer (7) is not stable in the sense of VDC ($s \in L_2 \cap L_\infty$, $s \rightarrow 0$) for such references; if moreover $\dot{s}$ is bounded, Tao's lemma [43] shows that $s \notin L_2$. For regulation the theorem is no obstruction: a motion that approaches a limit once has one

such error, which decays while the constraint stays active and supports the corrections, at the rate $\mu - \varrho_A$ if it is positive, for a nominal solution from $\mathcal{C}$ with $e_a = 0$ under Assumption 2 (Theorem 3).

Remark 2 (raising α_2). By (14) the error scales with $1/\alpha_{2,i}$ (Section VII-A: $\alpha_2 \max|s|$ between 1.31 and 1.45 m/s² for α_2 from 8 to 64 s⁻¹). A larger second rate lets the effort layer brake later and harder: it needs decelerations of the order of $\alpha_{2,i}$ times the approach speed within a time $1/\alpha_{2,i}$, which the sampling period, the bandwidth of the force loops and the effort bounds limit, and it needs the standoff σ_i to cover the mismatch through the margin $\alpha_{1,i}\alpha_{2,i}\sigma_i$. Rate consistency of the first layer provides a constructive design condition (Section V).

Remark 3 (the first layer alone). Without the effort layer, $\Delta \equiv 0$, and with exact feedforward, $e_a = 0$, the balance of a nominal solution with $K = kM$ is $\dot{S} = -2kS$, but safety then needs a velocity loop faster than the barrier: if $\|\nu_i\|_M \leq \bar{\nu}_i$ and $k > \alpha_{1,i}$, then $\tilde{h}_i(t) \geq e^{-\alpha_{1,i}t}(\tilde{h}_i(0) - \bar{\nu}_i\|s(0)\|_M/(k - \alpha_{1,i}))$, cf. the condition $\lambda > \alpha$ of [4, Thm. 3]; for $k < \alpha_{1,i}$ there are solutions from $\mathcal{C}$ that leave it (for $d = 1$, $h = q$, $u_n = 0$ and $u(0) = -\alpha_1 q(0) < 0$: $q(t) = q(0)(1 - \alpha_1(1 - e^{-kt})/k)$ as long as $q > 0$, which becomes negative). The effort layer removes this condition (Lemma 2), and Theorem 1 is its price when the first layer is of first order.

IV. THE SAFETY PORT

A. A dissipation inequality

Throughout this section $K = kM$, except in Remark 5. For $\beta \in \mathbb{R}$ define the *comparison efforts*

$$\varphi^{(\beta)} := \varphi_r - (k - \beta)\hat{s}, \quad (16)$$

so that $C\varphi^{(\beta)} = Ma_r + Nu_r + g - \hat{\tau}_e + \beta Ms$ under Assumption 2(b): the efforts of the law (3) with the gain k replaced by β ; their model acceleration is $a^{(\beta)} := a_r + M^{-1}Ns + \beta s$. Let $\Pi_j^{(\beta)} := G_j\varphi^{(\beta)} - r_j$ be the value of constraint j of $\mathcal{F}$ at these efforts. A set A of constraints *supports* the correction if all its constraints bind at φ and $\Delta = \sum_{j \in A} \lambda_j H^{-1}G_j^\top$ with $\lambda_j \geq 0$. The set of all binding constraints supports it, and every supporting set contains one with linearly independent gradients (Farkas' lemma and Carathéodory's theorem, for every binding pattern). For a supporting set A of barrier constraints let $s_\parallel$ be the M -orthogonal projection of s on $\text{span}\{\nu_i : i \in A\}$, $s_\perp := s - s_\parallel$, and

$$\mathfrak{d}_A[y] := \min\{\|d\|_M : J_i d \geq y_i \ (i \in A)\} \in [0, \infty], \quad (17)$$

the kinetic norm of the smallest acceleration that produces at least the rates y_i . It is monotone and subadditive, and $\mathfrak{d}_A[y] = 0$ for $y \leq 0$.

Theorem 2 (port inequality). *Let Assumptions 1 and 2(b) hold and consider a solution. For a.e. t and every $\beta \in \mathbb{R}$, with $\mu := \min\{k, \beta\}$:*

- (a) $P_f \leq (k - \mu)\|s\|_M^2 + \|s\|_M \text{dist}_H(\varphi^{(\beta)}, \mathcal{F})$;
- (b) *for every supporting set A of barrier constraints, $\mathfrak{d}_A^{(\beta)} := \mathfrak{d}_A[-\Pi_A^{(\beta)}] < \infty$ and*

$$P_f \leq (k - \mu)\|s\|_M^2 + \|s\|_M \mathfrak{d}_A^{(\beta)}; \quad (18)$$

- (c) *if the gradients of such a set are linearly independent, then with $w_A := (J_i s)_{i \in A}$ and $\Lambda_A := J_A M^{-1} J_A^\top$, $P_f = (k - \beta)\|s\|_M^2 + w_A^\top \Lambda_A^{-1} \Pi_A^{(\beta)}$;*
- (d) *with the multipliers of a supporting set A of barrier constraints, $P_f = \sum_{i \in A} \lambda_i (\psi_{1,i} - \tilde{z}_i)$.*

Part (a) is a comparison: if the efforts of the same law with the smaller gain β are admissible, the port takes back at most the share $(k - \beta)/k$ of the dissipation; with (5), $\dot{S} \leq -2\mu S + \sqrt{2S}(\text{dist}_H(\varphi^{(\beta)}, \mathcal{F}) + \|e_a - e_m\|_M)$ for every β . For $\beta = k$ these are the Cauchy–Schwarz bounds; for $\beta < k$ the effort layer caps the effective gain along the binding gradients. Part (d) says which constraints inject: a binding constraint puts power in only if the machine moves away from the limit faster than the required motion does, $\tilde{\psi}_{1,i} > \tilde{z}_i$. Parts (a)–(d) use only that the metric is kinetic; $K = kM$ enters through (5). For effort bounds and contact constraints in a supporting set the proof of (b) gives the same bound in the geometry of H , with entries $\Pi_j^{(\beta)}$ that are non-negative whenever the comparison efforts respect constraint j .

Remark 4 (effort-metric alignment). The kinetic metric aligns the velocity feedback with the effort-space representation of the safety-port pairing. Positive scalar multiples of a kinetic metric leave the minimizer of (10) unchanged. For a general effort metric this alignment can fail, allowing the filter to inject energy into the storage even while a constraint is active and there is no defect. For $d = m = 2$, $C = I$, $M = \text{diag}(1, 0.01)$, $k = 12$, $e_a = e_m = 0$, one active constraint ($\tilde{z} = \tilde{\dot{z}} = 0$, no curvature) with $\alpha_2 = 4$, gradient $J = (-1, 0.01)$ and $s = (1, -10)$, the Euclidean metric $H = I$ gives $\dot{S} = +12.2\|s\|_M^2$, the kinetic metric $\dot{S} = -7.21\|s\|_M^2$.

Remark 5 (the gain $K = kM$ is needed). For a symmetric $K \succ 0$ in (3), let $\bar{K} := M^{-1/2}KM^{-1/2}$ have the extreme eigenvalues $k_{\min} \leq k_{\max}$. The proof of Theorem 2(a) with the comparison efforts $\varphi_r - C^\sharp(K - \beta M)s$ and their H -distance δ_β to $\mathcal{F}$ gives $-s^\top Ks + P_f \leq -\mu_K\|s\|_M^2 + \|s\|_M \delta_\beta$ with $\mu_K := \frac{1}{2}(k_{\min} + \beta - \|\bar{K} - \beta I\|_2)$, which is $\min\{k, \beta\}$ for $K = kM$ and $\beta - \frac{1}{2}(k_{\max} - k_{\min})$ for $\beta \leq k_{\min}$. The loss is real: for $d = m = 2$, $M = C = H = I$, $K = \begin{bmatrix} 12 & 3.4 \\ 3.4 & 1 \end{bmatrix}$, one active constraint with $J = (1, 0)$, $\alpha_2 = 2$, no defect and $s = (-1, 1.7)$, one finds $\dot{S} = +0.23\|s\|_M^2$, while every $K = kM$ gives $\dot{S} \leq -\min\{k, \alpha_2\}\|s\|_M^2$ here by Theorem 3 (no defect, $\beta = \alpha_2$); e.g. $K = 12I$ gives $\dot{S} = -9.43\|s\|_M^2$.

B. The constraint identity

The defect $\mathfrak{d}_A^{(\beta)}$ is formed from the values of the supporting constraints at the comparison efforts. These values can be written in terms of the required motion. Let

$$\gamma_i := \dot{J}_i - J_i M^{-1}N, \quad \chi_i := \gamma_i s = \langle \nabla_t \nu_i, s \rangle_M,$$

where $\nabla_t \nu_i := \dot{\nu}_i + M^{-1}N\nu_i$ is a covariant derivative along the motion that is compatible with the kinetic metric ($\frac{d}{dt}\langle a, b \rangle_M = \langle \nabla_t a, b \rangle_M + \langle a, \nabla_t b \rangle_M$ by (2)). The *curvature term* χ_i vanishes when the constraint gradient is covariantly constant, $\nabla_t \nu_i = 0$; for the Christoffel factorization of N (with $M = M(q)$) and a time-invariant $h_i \in C^2$ it is the Hessian

of h_i in the kinetic metric, evaluated on (u, s) . The term χ_i is the geometric remainder in (19).

Lemma 3 (constraint identity). *Let Assumption 1 hold. Along every solution, a.e., for every barrier constraint i and every $\beta \in \mathbb{R}$, the value $\hat{\psi}_{2,i}(\varphi')$ at any efforts φ' with $\hat{a}(\varphi') = a^{(\beta)}$ (under Assumption 2(a),(b) this is $\Pi_i^{(\beta)}$, since $\hat{a}(\varphi^{(\beta)}) = a^{(\beta)}$) is*

$$\Pi_i^{(\beta)} = \dot{z}_i + \beta \tilde{z}_i + (\alpha_{2,i} - \beta) \tilde{\psi}_{1,i} - \chi_i - J_i e_a. \quad (19)$$

The identity is algebraic and holds for any absolutely continuous required velocity. A law of rate β drives $\tilde{\psi}_{1,i}$ towards $\tilde{z}_i$ at the rate β , while the effort constraint lets $\tilde{\psi}_{1,i}$ decrease at most at the rate $\alpha_{2,i}$. The two agree, up to curvature, if the slack does not close faster than at the rate β . We call

$$\zeta_i^{(\beta)} := [\dot{z}_i + \beta \tilde{z}_i]^-, \quad \eta_i^{(\beta)} := (\alpha_{2,i} - \beta) [\tilde{\psi}_{1,i}]^- \quad (20)$$

the *slack defect* and the *sign defect* of constraint i .

Theorem 3 (storage inequality). *Let Assumptions 1 and 2 hold and consider a solution. For a.e. t , every supporting set A of barrier constraints and every $\beta \leq \alpha_A := \min_{i \in A} \alpha_{2,i}$ ($\alpha_\emptyset := \infty$; for $A = \emptyset$, $s_\parallel = 0$ and $P_f = 0$), with $\mu = \min\{k, \beta\}$ and $\tau := \zeta^{(\beta)} + \eta^{(\beta)} + \chi$ (entries $i \in A$),*

$$\dot{S} \leq -k \|s_\perp\|_M^2 - \mu \|s_\parallel\|_M^2 + \|s_\parallel\|_M \mathfrak{d}_A[\tau] + \|s\|_M \|e_a\|_M - \langle s, e_m \rangle_M. \quad (21)$$

If $k < \beta \leq \alpha_A$, moreover

$$P_f \leq \frac{D_A^2}{4(\beta - k)}, \quad D_A := \mathfrak{d}_A[\tau] + \|e_a\|_M. \quad (22)$$

Further: (i) $\zeta_i^{(\beta)} = 0$ a.e. on the set of times at which constraint i is active; (ii) $\eta^{(\beta)} = 0$ on $\mathcal{C}$; (iii) if the gradients of A are linearly independent, then with the curvature rate $\varrho_A := \|\Lambda_A^{-1/2} \Gamma_A M^{-1/2}\|_2$, where Γ_A has the rows γ_i ,

$$\mathfrak{d}_A[\tau] \leq \|[\zeta^{(\beta)} + \eta^{(\beta)}]^+\|_{\Lambda_A^{-1}} + \varrho_A \|s\|_M. \quad (23)$$

For one constraint, $\varrho_A = \|\nabla_t \nu_i\|_M / \|\nu_i\|_M$.

Under the stated model and design assumptions, the inequality holds for every initial state. It shows that the effort layer does not act on the part $s_\perp$ of the velocity error orthogonal to the supporting gradients, and that along these gradients it costs at most the rate $k - \mu$ and an input whose only parts are the slack defect, the sign defect and the curvature term. For $k < \alpha_A$, (22) with $\beta = \alpha_A$ is quadratic in the defect and loses no rate. By (i), (ii) and (23), for a supporting set A with independent gradients and while its constraints are active in the first layer, for a nominal solution from $\mathcal{C}$ with $e_a = 0$ and with $\beta = \alpha_A$, $\mu = \min\{k, \alpha_A\}$, $\dot{S} \leq -2(\mu - \varrho_A)S$; for $k < \alpha_A$ also $\dot{S} \leq -2(k - \varrho_A^2/(4(\alpha_A - k)))S$. Active constraints are therefore harmless up to curvature. What remains is the slack defect, which is positive where the slack of a first-layer constraint closes faster than at the rate β : on the way into an activation, which is where Theorem 1 places the error.

V. RATE CONSISTENCY

Figure 2 connects the shared RoboCompiler interfaces and VDC body-storage assembly to the effort projection and reference-rate design. The kinetic effort metric links the safety correction to the tracking-storage balance. A feasible acceleration-level reference filter enforces $\dot{z}_i + \bar{\beta} \tilde{z}_i \geq 0$. With nonnegative initial slacks and $0 < \bar{\beta} \leq \min_i \alpha_{2,i}$, this removes the slack defect from the storage inequality. The resulting tracking estimates additionally depend on the stated model, correction-support and curvature hypotheses and the remaining defect terms.

A. A necessary and a sufficient condition

Exact tracking shows what the required motion must satisfy.

Proposition 1 (necessity). *Let Assumption 1 hold and let (q, u, u_r, φ) be as in Theorem 1, with $e_m = 0$. If $s = 0$ on an interval $I' \subset I$, then for every barrier constraint i , $\tilde{\psi}_{1,i} = \tilde{z}_i$ on I' and*

$$\dot{z}_i + \alpha_{2,i} \tilde{z}_i = \tilde{\psi}_{2,i} \geq 0 \quad \text{a.e. on } I'; \quad (24)$$

if the solution starts in $\mathcal{C}$, also $\tilde{z}_i \geq 0$ on I' . If (3) holds, then for a.e. t with $s(t) = 0$ (and $\hat{b}_i(t)$, $\hat{J}_i(t)$, $\hat{u}_r(t)$ defined) the nominal efforts have the values $\hat{\psi}_{2,i}(\varphi_r) = \dot{z}_i + \alpha_{2,i} \tilde{z}_i - J_i e_a$, for every gain K .

So a required motion can be followed exactly only if it satisfies the second-order constraints itself, and if it does and $e_a = 0$, the effort layer leaves the nominal efforts unchanged at $s = 0$ (when $\varphi_r \in \Phi$). The first layer (7) guarantees $\tilde{z}_i \geq 0$ and nothing about $\dot{z}_i$.

Definition 2 (rate consistency). Let $\bar{\beta} \geq 0$. Along a solution the required velocity is *consistent at the rate $\bar{\beta}$* if for every barrier constraint i , $\tilde{z}_i(t) \geq 0$ for all t and $\dot{z}_i + \bar{\beta} \tilde{z}_i \geq 0$ a.e.

Equivalently, $t \mapsto e^{\bar{\beta}t} \tilde{z}_i(t)$ is non-negative and non-decreasing: no slack closes faster than at the rate $\bar{\beta}$. A positive slack stays positive, so a constraint that is active at some time has been active since $t = 0$: consistency excludes the activations of Theorem 1, and the first layer approaches its limits asymptotically. By Proposition 1, consistency of constraint i at the rate $\alpha_{2,i}$ is necessary for $s \equiv 0$ along a nominal solution that starts in $\mathcal{C}$; along a nominal solution, a slack that closes faster than at the rate $\alpha_{2,i}$ on an interval excludes $s = 0$ there. The next theorem combines consistency at a rate $\bar{\beta} \leq \min_i \alpha_{2,i}$ with barrier-supported corrections and an explicit curvature bound. It establishes preservation of exact nominal tracking and provides a decay estimate when the resulting net dissipation rate is positive.

Theorem 4 (sufficiency). *Let Assumptions 1 and 2 hold, let $0 \leq \bar{\beta} \leq \alpha_{\min} := \min_{i \in \mathcal{I}} \alpha_{2,i}$, $\mu := \min\{k, \alpha_{\min}\}$, and consider a solution on $I = [0, T)$ whose required velocity is consistent at the rate $\bar{\beta}$.*

- (a) *For a.e. t and every non-empty supporting set A of barrier constraints (for $A = \emptyset$, $P_f = 0$), (21) and, for $k < \alpha_A$, (22) hold with $\beta = \alpha_A$ and without the slack defect: $\tau = \eta^{(\alpha_A)} + \chi$.*

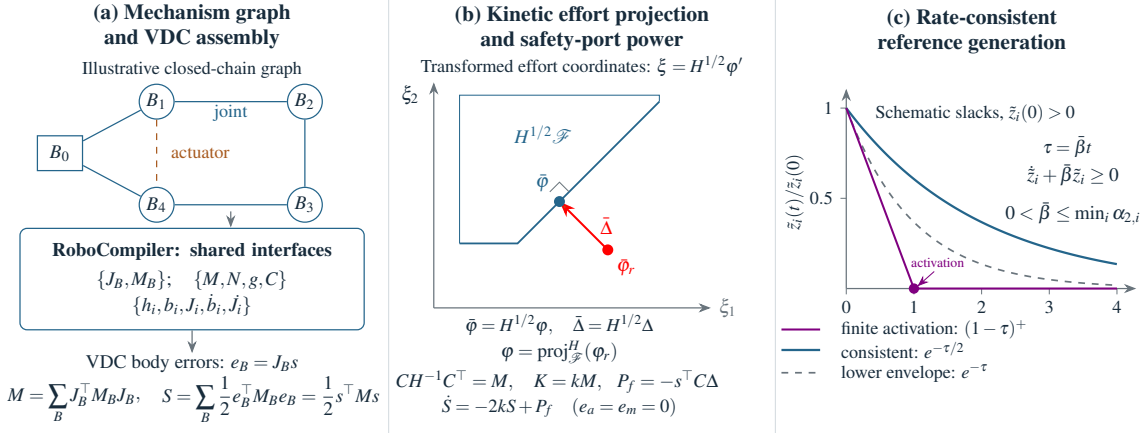


Fig. 2. Methodology and geometric interpretation. (a) An illustrative mechanism graph supplies the shared mechanical, actuator and barrier interfaces, while VDC body storages assemble into the kinetic tracking storage S . (b) An illustrative instantaneous two-dimensional effort projection in transformed coordinates $H^{1/2}\varphi'$. The correction Δ exchanges safety-port power $P_f = -s^\top C\Delta$ with the tracking storage. (c) Schematic normalized reference slacks contrast finite-time activation with rate-consistent evolution and its exponential lower envelope. The curves illustrate the design principle rather than simulation results.

- (b) Let the solution be nominal, start in $\mathcal{C}$ and have $e_a = 0$. Let the correction have a supporting set $A(t)$ of barrier constraints for a.e. t , and let $\varrho \geq 0$ be measurable and locally bounded with $\mathfrak{d}_{A(t)}[\chi] \leq \varrho(t)\|s(t)\|_M$ a.e. (Remark 6). Then

$$\|s(t)\|_M \leq \exp\left(-\int_0^t \omega \, d\tau\right) \|s(0)\|_M \quad (t \in I), \quad (25)$$

with $\omega := \mu - \varrho$ if $k \geq \alpha_{\min}$ and $\omega := \max\{\mu - \varrho, k - \varrho^2/(4(\alpha_{\min} - k))\}$ if $k < \alpha_{\min}$.

- (c) Let $A(t)$ and ϱ be as in (b), without the other hypotheses of (b), and let $\iota \geq \mathfrak{d}_{A(t)}[\eta^{(\alpha_{A(t)})}] + \|e_a\|_M + \|e_m\|_M$ be locally integrable (the first term is 0 where $A(t) = \emptyset$). Then $\|s(t)\|_M \leq e^{-\int_0^t (\mu - \varrho) dt'} \|s(0)\|_M + \int_0^t e^{-\int_\tau^t (\mu - \varrho) dt'} \iota(\tau) d\tau$ for $t \in I$.

Corollary 2 (exact tracking). *Under the hypotheses of Theorem 4(b), $s(0) = 0$ implies $s \equiv 0$ on I ; then $\hat{\psi}_{2,i}(\varphi_r) = \dot{z}_i + \alpha_{2,i} \tilde{z}_i \geq 0$ a.e. for every barrier constraint, and $\Delta = 0$ a.e.; in particular $\varphi_r = \varphi \in \Phi$ a.e. If all barrier constraints have the same second rate α_2 , a nominal solution that starts in $\mathcal{C}$ with $s(0) = 0$, has $e_a = 0$ and satisfies the hypotheses of Theorem 4(b) on the supporting sets and on ϱ has $s \equiv 0$ if and only if its required velocity is consistent at the rate α_2 .*

Remark 6 (curvature bounds). If for a.e. t the correction has a supporting set $A(t)$ of barrier constraints with $\Lambda_{A(t)} \succeq \lambda I$ for a constant $\lambda > 0$, then $\varrho(t) := \max\{\varrho_A(t) : A \subset \mathcal{I}, \Lambda_A(t) \succeq \lambda I\}$ is measurable, locally bounded and satisfies the hypothesis of Theorem 4(b) by (23) (with $\varrho_\emptyset := 0$). If $h_i \in C^2$ does not depend on t and N is linear in u (a time-invariant model of a mechanism on a fixed base), γ_i is linear in u ; if moreover $\|\Gamma_A M^{-1/2}\|_2 \leq \bar{\gamma}\|u\|_M$ and $\|u_r\|_M \leq \bar{u}_r$, then $\varrho \leq \bar{\gamma}(\bar{u}_r + \|s\|_M)/\sqrt{\lambda}$, and (25) holds with the constant rate $\mu - \bar{\gamma}(\bar{u}_r + \|s(0)\|_M)/\sqrt{\lambda}$ whenever it is positive, because $\|s\|_M$ then cannot exceed its initial value.

The reference rate $\bar{\beta}$ specifies the admissible required motions. The tracking rate is determined by the nominal dissipation and the curvature contribution. In particular, under

the hypotheses of Theorem 4(c), if $\mu - \varrho(t) \geq \omega_0 > 0$ a.e. and $\iota(t) \leq \bar{\iota}$, then

$$\|s(t)\|_M \leq e^{-\omega_0 t} \|s(0)\|_M + \frac{\bar{\iota}}{\omega_0} (1 - e^{-\omega_0 t}).$$

Thus zero defects give exponential decay, while bounded defects give an explicit ultimate error bound. If $M(t, q(t)) \succeq m_0 I$ uniformly for some $m_0 > 0$, the corresponding Euclidean error bound follows by dividing the right-hand side by $\sqrt{m_0}$.

B. A first layer on the required acceleration

Consistency is a condition on $\dot{u}_r$, so it can be imposed where $\dot{u}_r$ is chosen. Let the required velocity be a state of the controller,

$$\begin{aligned} \dot{u}_r &= a_r, \quad a_r = \arg \min_{a \in \mathbb{R}^d} \frac{1}{2} \|a - a_n\|_{Q_a}^2 \quad \text{s.t.} \\ J_i a &\geq -(\dot{b}_i + \dot{J}_i u_r + \alpha_{1,i} \dot{h}_i + \bar{\beta} \tilde{z}_i) \quad (i \in \mathcal{I}), \end{aligned} \quad (26)$$

with a metric $Q_a \in \mathbb{R}^{d \times d}$, $Q_a \succ 0$, a nominal acceleration a_n (for instance $a_n = \dot{u}_n + \kappa_r(u_n - u_r)$, $\kappa_r > 0$), the slacks $\tilde{z}_i = b_i + J_i u_r + \alpha_{1,i} \dot{h}_i$, and $\dot{b}_i$, $\dot{J}_i$, $\dot{h}_i$ formed along the measured motion.

Proposition 2 (acceleration-level first layer). *Along a motion on which (26) is feasible a.e. and a_r is locally integrable: (i) u_r is locally absolutely continuous and $e_a = 0$; (ii) $\dot{z}_i + \bar{\beta} \tilde{z}_i \geq 0$ a.e. and $\tilde{z}_i(t) \geq e^{-\bar{\beta} t} \tilde{z}_i(0)$, so if $\tilde{z}_i(0) \geq 0$ for all i , the required velocity is consistent at the rate $\bar{\beta}$ and satisfies the barrier constraints $\tilde{z}_i(u_r) \geq 0$ of (7) at all times; (iii) if $(q(0), u(0)) \in \mathcal{C}$, the choice $u_r(0) = u(0)$ gives $\tilde{z}_i(0) = \psi_{1,i}(0) \geq 0$ and $s(0) = 0$; (iv) for $a_n = \dot{u}_n + \kappa_r(u_n - u_r)$, with $\dot{u}_n$ the derivative of $u_n(t, q)$ along the motion, $\frac{d}{dt}(u_r - u_n) = -\kappa_r(u_r - u_n)$ on every interval on which no constraint of (26) binds.*

The constraints of (26) do not contain $\dot{u}$, so the required motion stays consistent whatever the effort layer and the plant do. By Corollary 2 and Proposition 2(iii), the loop with the first layer (26), $\bar{\beta} \leq \alpha_{\min}$, a start in $\mathcal{C}$ and $u_r(0) = u(0)$ has

$s \equiv 0$ and an inactive effort layer under the hypotheses of Theorem 4(b). Then the closed loop is the exponential CBF program of relative degree two with the rates $(\alpha_{1,i}, \bar{\beta})$ [6] on the required acceleration, followed by exact inverse dynamics; the content of the theorem is the perturbed case, in which the effort layer acts and safety rests on it. Existence needs no Lipschitz property of a minimizer, because u_r is a state:

Proposition 3 (existence). *Let Assumption 1 hold with τ_e continuous, $f = \varphi$ and $\hat{\tau}_e = \tau_e$, let $h_i \in C^2$, $u_n \in C^1$, Q_a , H , the constraints of Φ and a selection in (3) be continuous, and let $a_n = \dot{u}_n + \kappa_r(u_n - u_r)$ (or any a_n continuous in (t, q, u, u_r)). Let $\mathcal{O}$ be the set of states (t, q, u, u_r) at which the feasible sets of (26) and (10) both contain a point that satisfies all their constraints strictly (so Φ must be given by inequalities; equality constraints, such as bilateral contacts, have to be eliminated first). Then $\mathcal{O}$ is open, the closed loop $\dot{q} = u$, $\dot{u} = M^{-1}(C\varphi + \tau_e - Nu - g)$, $\dot{u}_r = a_r$ has a continuous right-hand side on $\mathcal{O}$, and through every point of $\mathcal{O}$ there is a solution, which can be continued until it leaves every compact subset of $\mathcal{O}$. These are nominal solutions in the sense of Definition 1, with $e_a = 0$.*

C. Two-sided limits: a statement in terms of the data

For a barrier family that consists of the two limits of every coordinate, feasibility, existence for all times and the hypotheses of Theorem 4 follow from the data. Feasibility of such box constraints for exponential CBF constraints is known [23], [24]; the point here is the combination with the storage inequality.

Theorem 5 (two-sided limits). *Let Assumptions 1 and 2 hold with a model that does not depend on t , $\Phi = \mathbb{R}^m$, $f = \varphi$ and $\hat{\tau}_e = \tau_e$ continuous. Let the barrier family consist of the limits $h_j^- = \underline{\ell}_j - \underline{\ell}_j$, $h_j^+ = \bar{\ell}_j - \underline{\ell}_j$ of d functions $\ell_j \in C^2(\mathcal{Q})$, with common rates $(\alpha_{1,j}, \alpha_{2,j})$ for the two limits of a pair and constant standoffs with $\bar{\ell}_j - \underline{\ell}_j > \sigma_j^- + \sigma_j^+$; let $B := \{q : \tilde{h}_j^\mp \geq 0 \ \forall j\} \subset \mathcal{Q}$ be compact and $L := \partial\ell/\partial q$ invertible on B . Let the required velocity be given by (26) with $0 < \bar{\beta} \leq \alpha_{\min} := \min_j \alpha_{2,j}$ and the data of Proposition 3, let $\mu := \min\{k, \alpha_{\min}\}$, and let*

$$\bar{\varrho} := \sup_{(q,u) \in \mathcal{C}} \frac{\|\Gamma M^{-1/2}\|_2}{\sqrt{\lambda_{\min}(LM^{-1}L^\top)}}, \quad \Gamma := \dot{L} - LM^{-1}N.$$

Then for every initial state with $(q(0), u(0)) \in \mathcal{C}$ and $\tilde{z}_j^\mp(0) \geq 0$: both programs are strictly feasible along every solution; a solution exists on $[0, \infty)$ and every solution can be continued to $[0, \infty)$; (q, u) stays in the compact set $\mathcal{C}$, u_r satisfies the barrier constraints of (7), and $\|s(t)\|_M \leq e^{-\underline{\omega}t}\|s(0)\|_M$, where $\underline{\omega} := \mu - \bar{\varrho}$ if $k \geq \alpha_{\min}$ and $\underline{\omega} := \max\{\mu - \bar{\varrho}, k - \bar{\varrho}^2/(4(\alpha_{\min} - k))\}$ if $k < \alpha_{\min}$. In particular $s \equiv 0$ if $s(0) = 0$, for every value of $\bar{\varrho}$.

Theorem 5 supplies existence, feasibility and safety directly from the coordinate-limit data, and exact tracking from $s(0) = 0$ for every finite $\bar{\varrho}$. A positive $\underline{\omega}$ additionally gives exponential decay. For other barrier families, Theorem 4 uses feasible programs and a trajectory-wise curvature bound (Section VIII).

Remark 7 (reference rate and implementation). A sufficient choice for per-constraint reference rates is $\max_{i \in A} \bar{\beta}_i \leq \min_{i \in A} \alpha_{2,i}$ on every supporting set A . The layer uses second-order barrier terms along the measured motion and selects the required acceleration through (26). A relaxation $\epsilon_i \geq 0$ of a constraint contributes the bounded slack defect $\zeta_i^{(\bar{\beta})} \leq \epsilon_i$ to (21). For $s = 0$ and a binding acceleration constraint, the nominal effort slack is $(\alpha_{2,i} - \bar{\beta})\tilde{z}_i$. Thus $\bar{\beta} < \alpha_{2,i}$ provides a positive margin whenever $\tilde{z}_i > 0$ and makes braking begin earlier; $\bar{\beta} = \alpha_{2,i}$ gives zero margin on that constraint. The reference gains $\bar{\beta}$ and κ_r have units s^{-1} .

VI. CONDITIONING AND REFERENCE TRACKING

Since $P_f = -\langle s, M^{-1}C\Delta \rangle_M$, the port and the feedforward defect enter (5) in the same way. If the required velocity is a controller state whose derivative contains the change $M^{-1}C\Delta$ of the model acceleration that the effort layer commands, the two cancel for every correction. A minimal form is

$$u_r = U + u_\Delta, \quad \dot{u}_\Delta = -\kappa u_\Delta + M^{-1}C\Delta, \quad a_r = \dot{U} - \kappa u_\Delta, \quad (27)$$

with the output U of a first layer and a rate $\kappa > 0$. This is the conditioning idea of anti-windup design [39], [44] and of pseudo-control hedging [40], where it keeps an adaptive law from responding to input limitations, applied to the passivity-based law.

Proposition 4 (conditioning). *Let Assumption 1 hold, and let $q, u, u_r, a_r, \varphi_r, f, \hat{\tau}_e$ be as in Definition 1, except that $\varphi = \varphi_r + \Delta$ with an arbitrary locally bounded measurable correction Δ ; define e_a^0 by $\dot{u}_r = a_r + M^{-1}C\Delta + e_a^0$ a.e. Then $M\dot{s} + Ns + Ks = M(e_a^0 - e_m)$ and $\dot{S} = -s^\top Ks + \langle s, e_a^0 - e_m \rangle_M$. Moreover, for (27) with $\kappa = k$, $K = kM$, $e_m = 0$, $\dot{U}$ exact and $s(0) = 0$: $s \equiv 0$, and $s^\circ := -u_\Delta$ satisfies $\dot{s}^\circ = -ks^\circ - M^{-1}C\Delta$ and $u = U - s^\circ$, whereas the loop of Section II with $a_r = \dot{U}$ has $u = U - s$ with $\dot{s} = -ks - M^{-1}Ns - M^{-1}C\Delta$, the nominal accelerations differing by the term $M^{-1}Ns$. For $N = 0$, the deviation systems have identical closed-loop equations after identifying s° with s , provided both use the same effort filter and actuator-allocation map from the nominal generalized force to φ_r ; for $m = d$, this allocation is unique.*

Conditioning preserves the storage balance by incorporating the effort correction into the required velocity. The deviation from the original reference is $u - U = u_\Delta - s$, and Theorem 1 applies with U as comparison velocity. Thus conditioning protects the modular storage certificate, whereas rate consistency addresses tracking of the reference produced by the first layer.

VII. NUMERICAL VALIDATION

A. Continuous-time illustrations

The continuous-time experiments isolate the tracking mechanism under the assumptions of the theory. The six-joint sample manipulator of Pinocchio 3.8.0 [37] has ideal torque sources, $K = kM$, and the kinetic effort metric $H = M^{-1}$. The constraints are $q_4 \leq 1.25$ rad, $-0.2 \leq q_2 \leq 1.5$ rad, and end-effector coordinates $z \geq 0.3$ m and $x \leq 1.7$ m, with

rates $(\alpha_1, \alpha_2) = (8, 20)$ for joints and $(6, 16)$ for Cartesian clearances (all rates in s^{-1}). The periodic reference is

$$q_d = Q_A + \frac{1}{2}(1 - \cos(2\pi t/3))(Q_B - Q_A),$$

where $Q_A = (0, 0.5, 0, 1, 0, 0.3)$ and $Q_B = (0.4, 0.9, 0, 1.4, 0.2, 0.3)$ rad; the plant starts at Q_A at rest and $u_n = \dot{q}_d + 12(q_d - q)$. The first-order layer has $Q_v = I$ and uses the exact one-sided derivative of u_r as feedforward. The consistent layer has $Q_a = I$, $\bar{\beta} = 16$, $\kappa_r = 20$ and $u_r(0) = u(0)$. RK4 steps are 1 ms; active-set changes are located by bisection and the integration step is split at the change.

Figure 3(a) shows a peak $\|s\|_M = 0.2350 \sqrt{J}$ for $k = 12$ and $0.2345 \sqrt{J}$ for $k = 30$, repeated over four periods. At floor activations, the effort constraint binds for 0.061 s, close to $1/\alpha_2 = 0.0625$ s. The left-hand side of Corollary 1 is 0.1598 and 0.1595 m/s for the two gains, against the bound 0.1595 m/s: agreement within 0.3%. At the elbow limit the slack closes at an increasing rate; the integral bound (12), evaluated from the start of the binding interval, is attained within 0.8%. The consistent layer gives $s \equiv 0$ for both gains, as predicted by Corollary 2. With an initial velocity error, the fitted decay rates are 12.25 and 29.9 s^{-1} ; Theorem 4(b) gives the respective bounds 12.00 and 15.76 s^{-1} using the measured curvature rate at most 0.24 s^{-1} . Initial required velocities for the decay runs are successive draws 0.8ξ , $\xi \sim \mathcal{N}(0, I_6)$, from NumPy generator seed 3, projected in the Euclidean metric onto $J_i(Q_A)u_r \geq -\alpha_{1,i}h_i(Q_A) + 0.02$ for all five barriers. Their initial kinetic errors are 8.226 and $5.236 \sqrt{J}$ for $k = 12$ and 30, respectively.

For the mismatch experiment, the plant acceleration is augmented by $e_m(t) = 0.3v(t)/\sqrt{6}$, where

$$v(t)^\top = (\sin 7t, \cos 5t, \sin(3t + 1), \cos 11t, \sin 13t, \cos 2t).$$

Thus $\|e_m\| \leq 0.3$, with standoffs $\sigma_i = 2.2(0.3)/(\alpha_{1,i}\alpha_{2,i})$ in the barrier coordinates, using the declared gradient-norm bound 2.2 for that run. The consistent layer's period peaks remain between 0.049 and $0.055 \sqrt{J}$.

Example 1 uses $u_n = 0.5 \sin(\pi t) - 0.1 \text{ m/s}$, $q(0) = 0.3 \text{ m}$, $u(0) = 0$, rates $(6, 16)$, and the exact one-sided feedforward derivative; RK4 steps are 0.2 ms for both layers with active-set localization. The first-order layer's period peaks are 0.0868–0.0869 m/s for $k = 12, 30, 100$ in periods 3–8. Corollary 1 is attained within 0.5%. Figure 4 contrasts this gain insensitivity with the dependence on the barrier rate: for $\alpha_2 = 8, 16, 32, 64 \text{ s}^{-1}$, the peaks are 0.163, 0.0869, 0.0447, 0.0226 m/s, and $\alpha_2 \max|s|$ lies between 1.31 and 1.45 m/s^2 . The consistent rate $\bar{\beta} = 16$ gives $s \equiv 0$ for all three gains. The smooth acceleration-level reference with $\bar{\beta} = 40$ has a recurring 0.054 m/s error, isolating the role of rate consistency beyond reference smoothness. Table I corroborates the algebraic storage and projection identities on constructed, random and robot-model instances.

B. Two hydraulic excavator case studies

Plants. Figure 5 shows the two MuJoCo plants compiled from mechanism graphs by RoboCompiler [36]: a Komatsu

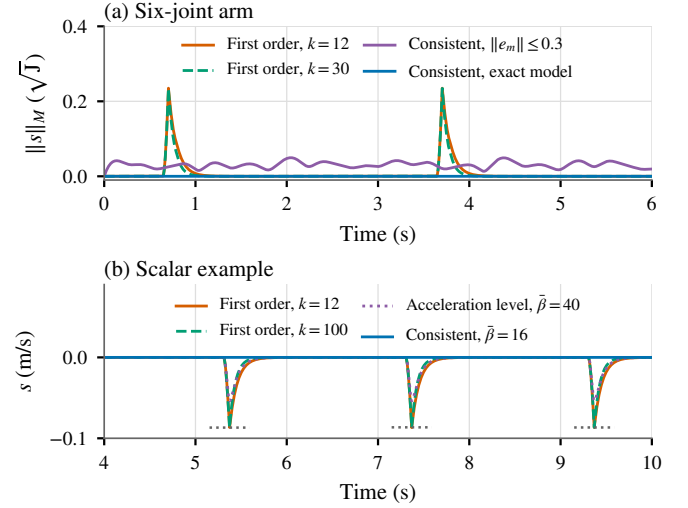


Fig. 3. Continuous-time illustrations. (a) Six-joint arm: with first-order CBF reference filtering, increasing the VDC gain leaves the onset peak essentially unchanged; the consistent layer tracks exactly in the nominal model and retains a small error under bounded acceleration mismatch. (b) Scalar example: the gain-independent activation error and the exact tracking obtained with the consistent rate. Dotted segments mark the instantaneous scalar error bound at each activation, including the preceding-error correction.

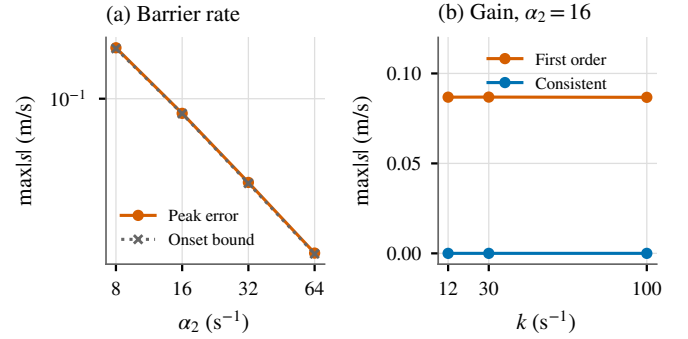


Fig. 4. Scalar illustration of the lower-bound mechanism. (a) Peak error and the measured onset bound decrease with α_2 . (b) Increasing the tracking gain k leaves the first-order CBF layer's recurring error unchanged; the consistent layer has zero error. Peaks are taken over periods 3–8.

tilt-rotator excavator with six independent coordinates and six actuator channels, and HEAP, with Menzi Muck M545 geometry from the RSL HEAP records [45], thirteen controlled coordinates, nineteen actuators and ten loop closures. These are explicitly parameterized simulation plants; the machine names identify the geometry sources. The native MuJoCo 3.3.7 plant [38] runs at 1 kHz with loop closures, compressible cylinder chambers, valve flow limits of 8 l/s per cylinder, leakage, relief and friction. Supply pressures are 25 MPa (Komatsu) and 30 MPa (HEAP). HEAP enforces anchored support points through Φ ; the plant uses 30 mm contact spheres, friction coefficient 0.8, normal impedance 0.5 and normal time constant 4 ms. Cylinder/linkage geometry and actuator coefficients are declared study parameters of the model records, which are not distributed.

VDC and CBF implementation. At $T_s = 10 \text{ ms}$, both variants use the assembled VDC law (3) with RoboCompiler's body modules, body gains kM_B with $k = 12$, and

TABLE I

INDEPENDENT NUMERICAL CHECKS OF THE ANALYTICAL IDENTITIES AND INEQUALITIES. IDENTITY RESIDUALS ARE RELATIVE TO $\max\{1, |x|\}$ OR $1 + |x|$ FOR A SIDE x ; (2) IS NORMALIZED BY THE LARGEST INERTIA ENTRY. INEQUALITY EXCESS IS NORMALIZED BY $\max\{1, |P_f|\}$ OR $1 + |\dot{S}|$. COMPILED-MODEL DERIVATIVES USE CENTRAL DIFFERENCES. THE PORT (B) TEST FAMILY INCLUDES 10 291 INSTANCES WITH DEPENDENT BINDING GRADIENTS.

Identity	Komatsu	HEAP
(2), 6 and 4 states	$3.36 \cdot 10^{-11}$	$1.24 \cdot 10^{-10}$
Storage balance	$6.68 \cdot 10^{-10}$	$2.67 \cdot 10^{-9}$
Constraint identity, 544 and 715 rows	$6.44 \cdot 10^{-11}$	$1.75 \cdot 10^{-10}$
Inequality / random or constructed instances		max. excess
Port (a): 29 467 instances, six rates		$4.1 \cdot 10^{-15}$
Port (b): 18 917 instances		$3.5 \cdot 10^{-12}$
Storage: 20 000 instances, three rates		$6.8 \cdot 10^{-13}$

(a) Komatsu



(b) HEAP



Fig. 5. MuJoCo case-study plants. (a) Komatsu tilt-rotator excavator. (b) HEAP walking excavator, including redundant actuation and support-contact constraints. Stills are taken from the accompanying comparison videos.

$u_n = J_x^{-1}(\dot{x}_d + 12(x_d - x))$. Here $x = x(q)$ is the task map, $x_d(t)$ its reference, and $J_x = \partial x / \partial q$ is square and nonsingular for the chosen independent task coordinates. A load observer has gain 100 s^{-1} . Stroke/joint barriers use $(\alpha_1, \alpha_2) = (8, 20)$, clearances $(6, 16)$, and virtual ceiling/wall barriers $(3, 16)$ and $(1.5, 20)$. Effort constraints apply to the predicted end-of-sample effort $f + \Theta(\varphi - f)$, where $\Theta = (1 - e^{-T_s/\tau})I$ and $\tau = 25 \text{ ms}$. The metric is $\Theta C^\top M^{-1} C \Theta$, augmented by a 10^{-3} null-space weight for HEAP. Declared force-model, load and sampling bounds determine the barrier standoffs [46]–[48]. The declared bounds are $0.5 \text{ kN}/0.15 \text{ kNm}$ for the tool wrench, 0.1 relative load error and 0.2 effectiveness error. Force-loop error bounds are 1% of channel capacity, with 0.25% for HEAP leg, tilt and rotation drives. The inter-sample row-variation bound is 2 in the corresponding barrier coordinates per s^3 . State-dependent margins are recomputed at each sample; the complete row-tightening formulas are in the accompanying `rcx/filter.py`. The declared error bounds are not uniformly satisfied in the logged runs. In the HEAP repeated-limit experiment, maximum boom force-prediction errors are 21.26 and 17.50 kN for the baseline and proposed layer, respectively, against a declared bound of 6.03 kN . There are 18 and 12 bound violations following barrier or support-contact intervention, respectively. The HEAP mission logs also contain force-prediction and load-bound violations. All

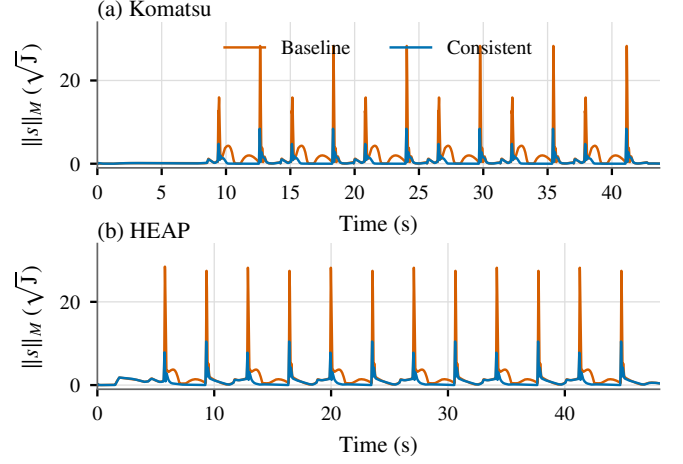


Fig. 6. Six repeated approaches to the boom stroke limit. The baseline’s onset and release peaks recur from cycle to cycle; the consistent layer reduces both for the two plants.

reported baseline and proposed runs pass the monitored row-residual checks and maintain positive monitored clearances. These results support the reported empirical performance but do not establish uniform satisfaction of the declared uncertainty bounds or certified intersample safety. The baseline uses (7); its feedforward adds a 30 ms first-order filtered difference quotient of $u_r - u_n$ to the nominal acceleration. The proposed hydraulic variant is a sampled approximation of the rate-consistent design (26), with $\bar{\beta}_i = \min\{16, \alpha_{2,i}\}$, $\kappa_r = 20$, and $u_r \leftarrow u_r + T_s a_r$; capability constraints act on a_r , and $\dot{J}_i u_r$ is evaluated as $\dot{J}_i u$. Both controllers therefore use the same RoboCompiler model, VDC controller and CBF effort layer, while the reference CBF layer determines the required motion’s rate and smoothness.

Repeated-limit experiment. Six cycles move the boom from an admissible pose toward a reference whose cylinder length is 40 mm beyond the extended stroke end, hold it for 0.5 s , and return. The declared limit is 30 mm inside the physical stroke end, so the unconstrained reference exceeds it by 70 mm . The comparisons are the baseline, the consistent layer, the first layer alone, and the smooth acceleration-level layer with $\beta = 40$. The latter separates reference smoothness from the rate condition $\beta \leq \alpha_2$. Table II reports peak storage, onset/return errors and positive energy contributions $E_j^+ = T_s \sum_\ell \max\{P_j(t_\ell), 0\}$, using the control-sample quadrature. The diagnostic powers are the safety port $P_f = -s^\top C(\varphi - \varphi_r)$, the force-loop defect $-s^\top C(f - \varphi)$, the sampled feedforward discrepancy $\langle s, \Delta u_r / T_s - a_r \rangle_M$, uncompensated load and zero-order hold. “Onset” denotes the largest $\|s\|_M$ in the six approach phases; “release” the largest in the return phases.

Activation mechanism. Figure 6 confirms recurring peaks in both plants, while Fig. 7 resolves the third cycle into velocity error, port power and stroke clearance. At the six stroke activations, the onset quantity $|J_i s(t_2)| + e^{-1}|J_i s(t_a)|$ is 1.061 – 1.064 (Komatsu) and 1.051 – 1.145 (HEAP) times $e^{-1}\tilde{z}_i(t_a)$. Thus the sampled hydraulic trajectories display the same onset mechanism identified by Theorem 1. Filtering and

TABLE II

SIX APPROACHES TO THE EXTENDED BOOM STROKE END ($k = 12$). LARGEST STORAGE; LARGEST VELOCITY ERROR ON THE WAY INTO THE LIMIT (ONSET) AND AFTER THE REFERENCE LEAVES IT (RELEASE); ENERGY THAT ENTERS THE STORAGE THROUGH EACH TERM OF ITS SAMPLED BALANCE (POSITIVE PARTS; “OTHER”: LOAD AND ZERO-ORDER HOLD) AND THE PORT SHARE; SMALLEST PLANT-SIDE CLEARANCE OF THE STROKE LIMIT (NEGATIVE: VIOLATED); SHARE OF SAMPLES WITH A BINDING BARRIER CONSTRAINT OF THE EFFORT LAYER; LARGEST RMS ERROR OF THE TASK COORDINATES NOT DRIVEN INTO THE LIMIT (HEAP: OF THE ARM, EXCEPT THE TELESCOPE). HEAP RETAINS THE GROUND-CONTACT CONSTRAINTS OF Φ IN ALL VARIANTS.

variant		$S_{\max}$ (J)	$\max\ s\ _M$ ($\sqrt{J}$)		energy into S (J)				port (%)	clear. (mm)	effort (%)	RMS (mrad)
			onset	release	port	feedfwd.	force loops	other				
Komatsu	first layer only	402	28.4	28.3	0	6763	5769	668	0	2.8	0	0.30
	baseline	401	15.9	28.3	1835	3788	3813	349	18.8	2.8	10.2	1.95
	raw feedforward	173	12.7	18.6	1006	280	2686	294	23.6	2.8	8.8	1.24
	acceleration level, $\bar{\beta} = 40$	36.8	8.58	8.40	340	280	786	144	21.9	2.8	35.2	0.81
	proposed	35.3	4.78	8.40	0.0063	99.3	797	149	<0.1	2.8	34.5	0.28
HEAP	first layer only	407	28.5	28.1	125	5844	6204	710	1.0	19.9	0	0.59
	baseline	405	28.5	27.5	490	5657	5996	873	3.8	20.1	12.3	0.70
	acceleration level, $\bar{\beta} = 40$	63.4	11.3	10.5	131	257	1749	504	5.0	20.0	34.1	0.63
	proposed	54.8	7.87	10.5	4.73	144	1462	398	0.2	20.0	34.3	0.59

force-loop lag also contribute at reference kinks: the first layer alone gives onset peaks 28.4 and 28.5 $\sqrt{J}$, compared with 15.9 and 28.5 for the baseline. The consistent layer reduces the baseline’s onset peaks by factors 3.3 and 3.6, and its positive port energy from 1835 to 0.0063 J and from 490 to 4.73 J, respectively. Minimum stroke clearances are preserved to within 0.1 mm: 2.8 mm for Komatsu and 20.0 mm for HEAP.

Smoothness and consistency. The $\bar{\beta} = 40$ variant has the same release errors as the consistent layer and storage peaks 36.8 and 63.4 J, compared with 35.3 and 54.8 J for the consistent layer and 401 and 405 J for the baseline. Smooth reference dynamics and acceleration feedforward therefore account for much of the storage reduction. Reducing only $\bar{\beta}$ from 40 to 16 yields an additional onset reduction of factors 1.8 and 1.4, and positive-port-energy reductions of approximately $5.4 \cdot 10^4$ and 28. Raw difference-quotient feedforward improves the Komatsu baseline to $S_{\max} = 173$ J, onset 12.7 $\sqrt{J}$ and port energy 1006 J; the consistent layer retains the smaller values in Table II. Conditioning (27) with $\kappa = k$ gives storage peaks 401 and 447 J and moves the port contribution into reference/feedforward terms, in agreement with Proposition 4.

Gain, rate and payload. Figure 8 and Table III show the Komatsu gain sweep $k = 2, 4, 6, 12, 24 \text{ s}^{-1}$. A twelvefold gain increase reduces the baseline’s onset peak by 33%, while its positive port energy increases by 59%. The consistent layer reduces onset error by factors 3.2–3.5 throughout the sweep. Its positive port energy is below 0.01 J for $k \geq 4$, and 5.03 J at $k = 2$, compared with 1465 J for the baseline. With bucket mass and inertia scaled by 1.5, onset error is 6.59 versus 17.7 $\sqrt{J}$ and port energy is 0.711 versus 2029 J. The effort layer alone maintains the limits with peaks 138 (Komatsu) and 196 $\sqrt{J}$ (HEAP); the first layer alone crosses the Komatsu declared limit by 0.4 mm at $k = 2$. Both two-layer variants maintain the standoff over the gain and payload runs.

With the consistent layer, effort barriers bind in 34.3–34.5% of the nominal cycle samples, compared with 10.2–12.3% for the baseline. The continuous-time design margin $(\alpha_{2,i} - \bar{\beta})\dot{z}_i$ approaches zero with the slack. In the implemented layer, the substitution $\dot{J}_i u_r \mapsto \dot{J}_i u$ contributes the residual $\dot{J}_i s$,

TABLE III

KOMATSU, THE SCENARIO OF TABLE II: GAIN k , RATE OF THE PROPOSED LAYER ($\bar{\beta}_i = \min\{16, \alpha_{2,i}\}$ UNLESS STATED), FIRST LAYER ALONE, AND A HEAVIER BUCKET. UNITS AND COLUMNS AS IN TABLE II; STROKE STANDOFF 2.8 MM.

variant	k	$S_{\max}$ (J)	$\max\ s\ _M$ onset	release	port (J)	clear. (mm)	effort (%)	RMS (mrad)
baseline	2	436	20.5	29.5	1465	3.7	2.9	5.66
baseline	12	401	15.9	28.3	1835	2.8	10.2	1.95
baseline	24	287	13.8	24.0	2334	2.8	11.4	1.35
proposed	2	51.5	6.26	10.1	5.03	2.8	18.4	1.23
proposed	12	35.3	4.78	8.40	0.0063	2.8	34.5	0.28
proposed	24	26.0	3.91	7.21	$<10^{-3}$	2.8	34.9	0.16
proposed, $\bar{\beta} = 8$	12	35.3	4.97	8.40	$<10^{-3}$	2.8	30.6	0.17
first layer only	2	650	36.1	29.5	0	-0.4	0	0.87
first layer only	12	402	28.4	28.3	0	2.8	0	0.30
bucket mass and inertia		1.5 times those of the model						
baseline	12	454	17.7	30.1	2029	3.0	6.5	2.80
proposed	12	50.4	6.59	10.0	0.711	3.0	31.4	1.83
first layer only	12	454	29.0	30.1	0	3.0	0	1.84

alongside sampling effects. The recorded binding fractions characterize these implemented loops. The small port energies are consistent with the pairing in Theorem 2(d): effort corrections exchange little tracking-storage energy when s is small. Mean offline Python computation times per update are comparable: 17.10/17.19 ms (Komatsu) and 31.80/31.59 ms (HEAP), baseline/consistent; simulations advance on a fixed plant clock.

Workspace constraints and missions. Table IV covers references into virtual walls and self-collision geometries. The consistent layer reduces positive port energy by factors 14–190 and peak storage by factors 2.1–7.9, with minimum clearances within 0.7 mm and task RMS errors equal or smaller. The dig-and-level missions in Table V include soil excavation with an embedded pipe obstacle, loading and levelling, and, for Komatsu, travel. Both controllers complete all phases in 397 s (Komatsu) and 406 s (HEAP), with positive minimum clearances 35.3 and 32.0 mm. The consistent layer reduces peak storage by factors 1.4–1.6 and positive port energy by factors 5.9–9.1. Excavated volumes differ by 0.25% and 1.2%, respectively. The baseline and consistent QPs remain

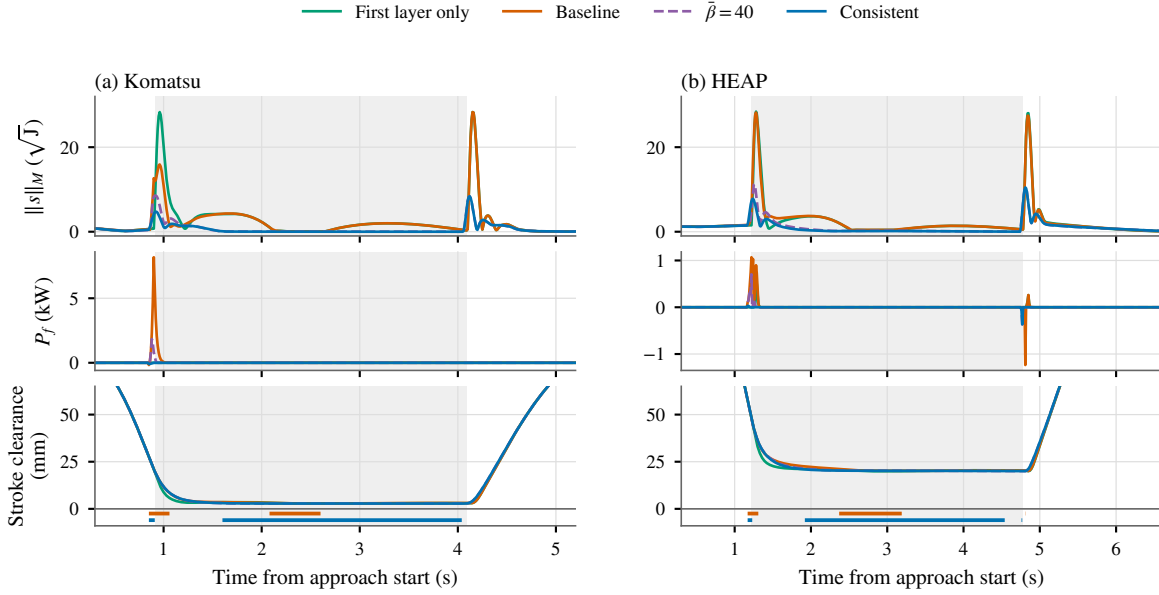


Fig. 7. Third cycle in the two excavator plants. Top: kinetic velocity error; middle: safety-port power; bottom: plant-side stroke clearance. Shading marks the baseline first-layer constraint's active interval. Bands below zero mark binding effort-barrier samples (orange: baseline; blue: consistent); zero is the declared stroke limit. The smooth $\bar{\beta} = 40$ variant suppresses the release peak, while the consistent rate further suppresses the onset peak and port injection.

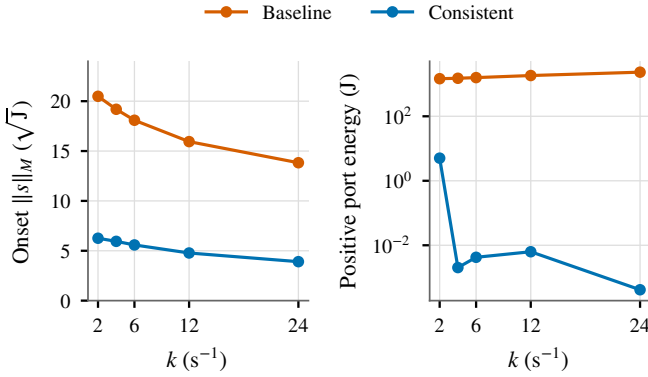


Fig. 8. Komatsu VDC gain sweep. Raising the tracking gain gives a modest onset improvement in the baseline and increases positive port energy. The consistent layer maintains a smaller onset error throughout the sweep and strongly reduces port injection.

feasible at every sample in the reported cycle, workspace and mission runs.

Reproducibility. The code packages at <https://github.com/Mehdi-Heydari-Shahna/RateConsistentCBF> provide the Pinocchio illustrations, the MuJoCo excavator benchmark and controllers, scenario references, logged results and analysis scripts; the two excavator model records are not distributed. Figure trajectories are available as CSV files. Videos compare the baseline and consistent controller side by side for the repeated-limit experiments and excerpts of the missions. Numerical sensitivity was observed in the Komatsu experiments. Two QP versions differing in their treatment of round-off directions produced proposed-layer mission port energies of 95.0 and 83.5 J, a difference of approximately 14 % relative to the smaller value, and changed e-fence entries by up to 3.5 %.

TABLE IV

FURTHER SCENARIOS WHOSE REFERENCES VIOLATE THE LIMITS: BASELINE (FIRST-ORDER FIRST LAYER) AND PROPOSED LAYER. E-FENCE: VIRTUAL WALLS AND CEILING AROUND THE WORKSPACE; SELF-COLL.: BUCKET AGAINST THE TRACK, THE BOOM OR THE WHEELS. CLEARANCE: SMALLEST PLANT-SIDE CLEARANCE OF THE PAIRS OF THE SCENARIO; RMS: LARGEST RMS TASK ERROR OVER THE JOINT COORDINATES, DOMINATED BY THE PARTS OF THE REFERENCES THAT THE LIMITS FORBID. NO LIMIT WAS VIOLATED.

		$S_{\max}$ (J)		port (J)		clear. (mm)		RMS (mrad)	
		base	prop.	base	prop.	base	prop.	base	prop.
Komatsu	e-fence	177	22.4	343	1.82	77.4	76.7	243.3	241.9
Komatsu	self-coll.	48.4	22.5	83.5	5.89	67.1	67.0	60.1	58.2
HEAP	e-fence	337	74.0	31.0	0.176	100.9	100.7	269.2	268.7
HEAP	self-coll.	36.8	6.76	31.8	0.800	93.2	92.5	107.2	106.6

VIII. DESIGN IMPLICATIONS

VDC certificate and CBF design. The lower bound and necessity result apply to every nominal effort law. The dissipation and sufficiency results specialize the design to $K = kM$ and $CH^{-1}C^T = M$; Remarks 4 and 5 show why these choices align the velocity feedback with the geometry of the effort projection. Theorem 2(a) remains available for the complete feasible set, including actuator and contact constraints, whereas Theorem 4(b) gives its sharper decay certificate when barrier constraints support the correction. Capability constraints on a_r coordinate the reference with actuator authority; conditioning (Section VI) provides a complementary storage-balance interface.

Curvature and margin selection. A trajectory-wise curvature bound makes Theorem 4 directly interpretable. For the arm of Section VII-A, the measured rate is below 0.24 s^{-1} , against $\mu = 12 \text{ s}^{-1}$. Sampling the full coordinate safe set gives lower estimates of its worst-case supremum of 80 s^{-1} for limits $\pm 0.5 \text{ rad}$ about Q_A and $9.1 \cdot 10^3 \text{ s}^{-1}$ for the model

TABLE V

DIG-AND-LEVEL MISSIONS (SOIL MODEL, DIGGING, LOADING, LEVELLING): DURATION, LARGEST STORAGE, ENERGY INTO THE STORAGE PER TERM OF ITS SAMPLED BALANCE (POSITIVE PARTS; "OTHER": LOAD AND ZERO-ORDER HOLD), PORT SHARE, SMALLEST PLANT-SIDE CLEARANCE OVER ALL PAIRS, VIOLATED PAIRS, EXCAVATED VOLUME AT THE END. ALL MISSIONS COMPLETED.

Metric	Komatsu		HEAP	
	baseline	proposed	baseline	proposed
Duration T (s)	397	397	406	406
Largest storage $S_{\max}$ (J)	118.8	84.1	90.3	57.4
Port energy (J)	556.9	95.0	190.8	21.0
Feedforward energy (J)	1679	130	513	130
Force-loop energy (J)	1606	819	1465	1251
Other energy (J)	7593	6148	10399	9965
Port share (%)	4.9	1.3	1.5	0.2
Minimum clearance (mm)	35.3	35.3	32.0	32.0
Violated pairs	none	none	none	none
Excavated volume (m ³)	0.526	0.527	0.501	0.507

limits ± 3.14 rad. For the continuous-time arm benchmark, the trajectory-wise rate gives the decay comparison for the reported motions. The proposed arm reference has mean task error 0.0435 rad against 0.0434 rad for the baseline, illustrating earlier braking with similar task accuracy. A choice $\bar{\beta} < \alpha_{2,i}$ provides the nominal effort slack $(\alpha_{2,i} - \bar{\beta})\tilde{z}_i$ (Remark 7).

RoboCompiler interfaces and implementation. RoboCompiler supplies the model and geometric derivatives shared by the VDC body modules and both CBF layers. The assembled VDC storage connects these interfaces to the safety-port inequality; the continuous-time results separate the slack, curvature and mismatch contributions explicitly. Force-loop and load-estimation errors enter e_m and the safety margin of Lemma 2; feedforward errors enter e_a . An inertia-model error also changes the gain and metric, so the certificate is evaluated using the stated inertia relation. The heavier-bucket experiment in Table III tests this sensitivity empirically. The sampled case studies use end-of-sample effort prediction, analytic barrier derivatives and standoffs for declared force, load and sampling error bounds. For the hydraulic acceleration layer, define the instantaneous implemented row residual

$$\mathcal{R}_i := J_i a_r + \dot{b}_i + \dot{J}_i u + \alpha_{1,i} \dot{h}_i + \bar{\beta}_i \tilde{z}_i.$$

Along an absolutely continuous reference reconstruction,

$$\dot{\tilde{z}}_i + \beta \tilde{z}_i = \mathcal{R}_i + (\beta - \bar{\beta}_i)\tilde{z}_i + \dot{J}_i s + J_i e_a$$

a.e.; hence

$$\zeta_i^{(\beta)} = [\mathcal{R}_i + (\beta - \bar{\beta}_i)\tilde{z}_i + \dot{J}_i s + J_i e_a]^-.$$

Where $\mathcal{R}_i \geq 0$, $\tilde{z}_i \geq 0$ and $\beta \geq \bar{\beta}_i$, this gives

$$\zeta_i^{(\beta)} \leq |\dot{J}_i s| + |J_i e_a|.$$

This identity relates the implemented reference approximation to the slack and feedforward defects of Theorem 3 under its continuous-time hypotheses. The hydraulic tables quantify the performance of the reported sampled implementation. Piecewise smooth obstacle primitives are evaluated on their smooth branches. The code and videos expose the resulting clearance, tracking and energy signals alongside each other, providing reproducible evidence for the implemented sampled loops.

IX. CONCLUSION

First-order reference filtering and second-order safety enforcement can impose incompatible constraint-approach rates. The resulting reference-slack dynamics yield a controller-independent tracking-error lower bound and, under uniform repeated-activation conditions, preclude convergence of the kinetic tracking error. A kinetic-metric projection inequality connects effort corrections to the VDC tracking storage. Rate-consistent reference generation removes the slack-closing defect and, under the stated support and curvature hypotheses, preserves exact initial nominal tracking and yields explicit decay and disturbance bounds. For two-sided coordinate limits with a nonsingular coordinate-limit Jacobian on a compact admissible configuration set and unconstrained efforts, strict feasibility and global continuation are established under nominal actuation. RoboCompiler supplies the shared mechanical interfaces. Continuous-time benchmarks illustrate the analytical predictions, while sampled hydraulic excavator simulations show reduced approach errors and positive safety-port energy with comparable clearances.

APPENDIX A PROOFS

A. Two lemmas on projections and kinetic metrics

Lemma 4 (projection). *Let $\langle \cdot, \cdot \rangle$ be an inner product on $\mathbb{R}^m$, $\mathcal{X} \subset \mathbb{R}^m$ non-empty, closed and convex, x^* the point of $\mathcal{X}$ nearest to x_0 , and $\Delta^* = x^* - x_0$. (i) For every $x^b \in \mathcal{X}$, with $\Delta^b = x^b - x_0$, one has $\|\Delta^*\|^2 \leq \langle \Delta^*, \Delta^b \rangle$, and for every v*

$$-\langle v, \Delta^* \rangle \leq -\frac{1}{2}\langle v, \Delta^b \rangle + \frac{1}{2}\|v\|\|\Delta^b\|. \quad (28)$$

(ii) *Let $\mathcal{X} = \{x : G_j x \geq r_j\}$ with finitely many constraints and gradients $\mathbf{g}_j$ ($\langle \mathbf{g}_j, x \rangle = G_j x$), and let A support Δ^* : its constraints bind at x^* and $\Delta^* = \sum_{j \in A} \lambda_j \mathbf{g}_j$ with $\lambda_j \geq 0$. The binding constraints support Δ^* , and every supporting set contains one with independent gradients. For a supporting set A , with $\mathcal{X}_A := \{x : G_j x \geq r_j, j \in A\}$ and the orthogonal projections v_A , Δ_A^b on $\mathcal{G}_A := \text{span}\{\mathbf{g}_j : j \in A\}$, x^* is the point of $\mathcal{X}_A$ nearest to x_0 , and for every $x^b \in \mathcal{X}_A$, $-\langle v, \Delta^* \rangle \leq -\frac{1}{2}\langle v_A, \Delta^b \rangle + \frac{1}{2}\|v_A\|\|\Delta_A^b\|$.*

Proof. (i) The variational inequality $\langle x_0 - x^*, x - x^* \rangle \leq 0$ ($x \in \mathcal{X}$) with $x = x^b$ gives $\langle \Delta^*, \Delta^b - \Delta^* \rangle \geq 0$, i.e. $\|\Delta^* - \frac{1}{2}\Delta^b\| \leq \frac{1}{2}\|\Delta^b\|$; write $-\langle v, \Delta^* \rangle = -\frac{1}{2}\langle v, \Delta^b \rangle - \langle v, \Delta^* - \frac{1}{2}\Delta^b \rangle$ and use Cauchy-Schwarz. (ii) That Δ^* lies in the cone generated by the binding gradients is Farkas' lemma (affine constraints), and a representation with independent gradients exists by Carathéodory's theorem for cones. For $x \in \mathcal{X}_A$, $\langle x_0 - x^*, x - x^* \rangle = -\sum_{j \in A} \lambda_j (G_j x - r_j) \leq 0$, so x^* is the nearest point of $\mathcal{X}_A$; since $\Delta^* \in \mathcal{G}_A$, (i) applied to $\mathcal{X}_A$ gives $\|\Delta^*\|^2 \leq \langle \Delta^*, \Delta_A^b \rangle$, and $-\langle v, \Delta^* \rangle = -\langle v_A, \Delta^* \rangle$ is estimated as in (i). $\square$

Lemma 5 (kinetic metrics). *Let $M \succ 0$ and $\text{rank } C = d$. (i) If $R_0 \succeq 0$, $R_0 C^\top = 0$ and $H = C^\top M^{-1} C + R_0 \succ 0$, then $CH^{-1}C^\top = M$. A matrix $H \succ 0$ is kinetic if and only if $R_0 := H - C^\top M^{-1} C$ satisfies $R_0 H^{-1} C^\top = 0$, and then $R_0 \succeq 0$. For $m = d$ the only kinetic metric is $C^\top M^{-1} C$.*

(ii) If H is kinetic and $C^\sharp = H^{-1}C^\top M^{-1}$, then $CC^\sharp = I$, $\langle C^\sharp y, \Delta \rangle_H = y^\top M^{-1}C\Delta$ and $\|C^\sharp y\|_H = \|y\|_{M^{-1}}$.

Proof. (i) $Y := C^\top(CC^\top)^{-1}M$ satisfies $HY = C^\top$, so $CH^{-1}C^\top = CY = M$. If H is kinetic, then $R_0H^{-1}C^\top = C^\top - C^\top M^{-1}CH^{-1}C^\top = 0$, and $R_0 \succeq 0$ because $C^\top(CH^{-1}C^\top)^{-1}C \preceq H$; conversely, $R_0H^{-1}C^\top = 0$ gives $C^\top = C^\top M^{-1}CH^{-1}C^\top$, and multiplying by $(CC^\top)^{-1}C$ from the left gives $CH^{-1}C^\top = M$. For $m = d$, C is invertible. (ii) is direct. $\square$

With $\hat{s} = C^\sharp Ms$, (ii) gives (11): $\langle \hat{s}, \Delta \rangle_H = s^\top C\Delta$, $\|\hat{s}\|_H = \|s\|_M$, and $G_i \hat{s} = J_i M^{-1}CC^\sharp Ms = J_i s$. For a barrier constraint $H^{-1}G_i^\top = C^\sharp M\nu_i$, and $x \mapsto C^\sharp Mx$ is an isometry from $(\mathbb{R}^d, \|\cdot\|_M)$ into $(\mathbb{R}^m, \|\cdot\|_H)$ that preserves inner products.

B. Proofs of Sections II and III

Lemma 1. $\dot{s} = e_a - M^{-1}(N + K)s - M^{-1}C\Delta - e_m$, and by (2) $\dot{S} = s^\top M\dot{s} + \frac{1}{2}s^\top(N + N^\top)s = s^\top M\dot{s} + s^\top Ns$.

Lemma 2. $\tilde{\psi}_{2,i} = \hat{\psi}_{2,i}(\varphi) + J_i e_m \geq -\varepsilon_i$ a.e., and $\frac{d}{dt}(e^{\alpha_{2,i}t}\tilde{\psi}_{1,i}) = e^{\alpha_{2,i}t}\tilde{\psi}_{2,i}$; integration from $\tilde{\psi}_{1,i}(0) \geq 0$ gives $\tilde{\psi}_{1,i} \geq -\varepsilon_i/\alpha_{2,i}$, and the same argument for $\tilde{h}_i + \alpha_{1,i}\tilde{h}_i = \tilde{\psi}_{1,i}$ gives $\tilde{h}_i \geq -\varepsilon_i/(\alpha_{1,i}\alpha_{2,i})$; $\varepsilon_i = 0$ gives the invariance.

Theorem 1. Since $e_m = 0$, $\tilde{\psi}_{2,i} = \hat{\psi}_{2,i}(\varphi) \geq 0$ a.e., with equality where the effort constraint binds, and $\frac{d}{dt}(e^{\alpha_{2,i}t}\tilde{\psi}_{1,i}) = e^{\alpha_{2,i}t}\tilde{\psi}_{2,i}$; integration over $[t_a, t_2]$ gives the first claim. If constraint i is active at t_2 , then $w_i(t_2) = -\tilde{\psi}_{1,i}(t_2)$ by (8), and $\tilde{\psi}_{1,i}(t_a) = \tilde{z}_i(t_a) - w_i(t_a)$, which gives (12). Moreover $|w_i| = |\langle \nu_i, s \rangle_M| \leq \|\nu_i\|_M \|s\|_M$. (i) If both norms were smaller than $X := \tilde{z}_i(t_a)/(\bar{v}(e^{\alpha_{2,i}\theta} + 1))$, (12) would give $\bar{v}X > e^{-\alpha_{2,i}\theta}(\tilde{z}_i(t_a) - \bar{v}X)$, i.e. $X > X$. (ii) Apply (i) with $t_2 = t_n$ and $t_a = t_n - \theta_n \rightarrow \infty$.

Corollary 1. By (12) with $\theta = 1/\alpha_{2,i}$, $|J_i s(t_2)| \geq -J_i s(t_2) \geq e^{-1}\tilde{z}_i(t_a) - e^{-1}J_i s(t_a) \geq e^{-1}\tilde{z}_i(t_a) - e^{-1}|J_i s(t_a)|$. If $\tilde{z}_i \leq -v$ a.e. on $[t_2 - \theta, t_2]$, then $\tilde{z}_i(t_2 - \theta) \geq v\theta$ because $\tilde{z}_i(t_2) = 0$, and $\theta \mapsto v\theta e^{-\alpha_{2,i}\theta}$ has its maximum $v/(e\alpha_{2,i})$ at $\theta = 1/\alpha_{2,i}$.

Remark 1. Put $t_a = t_2 - 1/\alpha_{2,i}$ and $x = \alpha_{2,i}(t - t_a)$, so that $\tilde{z}_i = (v/\alpha_{2,i})(1 - x)$ for $t \leq t_2$. While $s = 0$, (19) with $\beta = k$, $\chi_i = 0$ and $e_a = 0$ gives the value $\tilde{z}_i + \alpha_{2,i}\tilde{z}_i = -vx$ of the effort constraint at φ_r , which is negative exactly for $t > t_a$. From t_a on, the binding constraint gives $\tilde{\psi}_{1,i} = e^{-x}\tilde{z}_i(t_a) = (v/\alpha_{2,i})e^{-x}$ and $w_i = \tilde{z}_i - \tilde{\psi}_{1,i} = (v/\alpha_{2,i})(1 - x - e^{-x})$, and by (19) the value at φ_r is $\Pi_i^{(k)} = (v/\alpha_{2,i})[\alpha_{2,i}(e^{-x} - 1) + k(1 - x - e^{-x})] < 0$ for $x \in (0, 1]$ and every $k > 0$. This is the motion: with $\gamma_i = 0$, $e_a = e_m = 0$ and $K = kM$, $\dot{w}_i = \gamma_i s - kw_i - G_i \Delta$ and $G_i \Delta = [-\Pi_i^{(k)}]^+$, since constraint i alone supports the correction; by (19), $\Pi_i^{(k)}$ is affine in w_i for the given slack, so the right side is Lipschitz in w_i , and the function w_i above, which solves this equation with $w_i(t_a) = 0$, is its only solution. So the constraint binds on $(t_a, t_2]$, $|J_i s(t_2)| = \tilde{\psi}_{1,i}(t_2) = v/(e\alpha_{2,i})$, and $J_i s(t_a) = 0$.

C. Proofs of Section IV

Theorem 2. The command is the H -nearest point of $\mathcal{F}$ to φ_r ; apply Lemma 4 with $x_0 = \varphi_r$, $\Delta^* = \Delta$, $v = \hat{s}$, so

that $-\langle v, \Delta^* \rangle = P_f$. (a) Let δ have the smallest H -norm with $\varphi^{(\beta)} + \delta \in \mathcal{F}$ and put $\Delta^b = -(k - \beta)\hat{s} + \delta$. By (28), $P_f \leq \frac{1}{2}(k - \beta)\|\hat{s}\|^2 - \frac{1}{2}\langle \hat{s}, \delta \rangle + \frac{1}{2}\|\hat{s}\|(\|k - \beta\|\|\hat{s}\| + \|\delta\|) \leq [k - \beta]^+ \|s\|_M^2 + \|s\|_M \|\delta\|_H$, and $[k - \beta]^+ = k - \mu$. (b) The set $\{\delta : G_i \delta \geq -\Pi_i^{(\beta)}, i \in A\}$ contains $\Delta + (k - \beta)\hat{s}$ (the constraints of A bind at φ), so $\mathfrak{d}_A^{(\beta)} < \infty$; its element of smallest norm lies in $\mathcal{G}_A$. With $\Delta^b = -(k - \beta)\hat{s} + \delta \in \mathcal{X}_A - \varphi_r$, Lemma 4(ii) gives (b) as in (a), with $\hat{s}_A$ in place of $\hat{s}$; by the isometry, $\hat{s}_A = C^\sharp Ms_\parallel$, $\|\hat{s}_A\|_H = \|s_\parallel\|_M$, and an element $\delta = C^\sharp Md$ of $\mathcal{G}_A$ has $\|\delta\|_H = \|d\|_M$ and $G_i \delta = J_i d$. (c) $\Delta = C^\sharp Md$ with $d = M^{-1}J_A^\top \lambda$, and binding gives $\Lambda_A \lambda = -\Pi_A^{(k)}$, so $P_f = -s^\top Md = w_A^\top \Lambda_A^{-1} \Pi_A^{(k)}$; moreover $\Pi_A^{(k)} = \Pi_A^{(\beta)} + (k - \beta)w_A$ and $w_A^\top \Lambda_A^{-1} w_A = \|s_\parallel\|_M^2$. (d) $P_f = -\sum_i \lambda_i G_i \hat{s} = -\sum_i \lambda_i w_i$ and $w_i = \tilde{z}_i - \tilde{\psi}_{1,i}$.

Remark 5. Since $CC^\sharp = I$, the efforts $\varphi^b := \varphi_r - C^\sharp(K - \beta M)s$ have the model acceleration $a^{(\beta)}$. Lemma 4(i) with $\Delta^b = -C^\sharp(K - \beta M)s + \delta$, where δ is the H -smallest with $\varphi^b + \delta \in \mathcal{F}$, and Lemma 5(ii) give $P_f \leq \frac{1}{2}s^\top(K - \beta M)s + \frac{1}{2}\|s\|_M\|(K - \beta M)s\|_{M^{-1}} + \|s\|_M \delta_\beta$. With $x = M^{1/2}s$, $s^\top Ks \geq k_{\min}|x|^2$ and $\|(K - \beta M)s\|_{M^{-1}} = |(\bar{K} - \beta I)x| \leq \|\bar{K} - \beta I\|_2|x|$, which gives the bound. In the example, $\tilde{z} = \dot{\tilde{z}} = 0$ and $\tilde{\psi}_1 = -Js = 1$; since $\hat{a}(\varphi_r) = a^{(0)} + M^{-1}Ks$, (19) with $\beta = 0$ gives the value $\alpha_2\psi_1 + JKs = -4.22$ at φ_r , so $\Delta = 4.22 J^\top$, $P_f = 4.22$, $s^\top Ks = 3.33$ and $\|s\|^2 = 3.89$; for $K = 12I$ the value is -10 , $P_f = 10$ and $s^\top Ks = 46.68$.

Lemma 3. By (9), $\Pi_i^{(\beta)} = J_i a_r + J_i M^{-1}Ns + \beta w_i + \dot{J}_i u + \dot{b}_i + (\alpha_{1,i} + \alpha_{2,i})\dot{h}_i + \alpha_{1,i}\alpha_{2,i}\dot{\tilde{h}}_i$. Along the solution $\dot{\tilde{z}}_i = \dot{b}_i + J_i \dot{u}_r + \dot{J}_i u_r + \alpha_{1,i}\dot{\tilde{h}}_i$, and by (8) $\beta \tilde{z}_i + (\alpha_{2,i} - \beta)\tilde{\psi}_{1,i} = \alpha_{2,i}\dot{\tilde{h}}_i + \alpha_{1,i}\alpha_{2,i}\dot{\tilde{h}}_i + \beta w_i$. Subtracting, $\dot{\tilde{z}}_i + \beta \tilde{z}_i + (\alpha_{2,i} - \beta)\tilde{\psi}_{1,i} - \Pi_i^{(\beta)} = J_i(\dot{u}_r - a_r) + \dot{J}_i s - J_i M^{-1}Ns = J_i e_a + \chi_i$. By (2), $\dot{\nu}_i = M^{-1}J_i^\top - M^{-1}(N + N^\top)\nu_i$, so $\langle \nabla_t \nu_i, s \rangle_M = \dot{J}_i s - \nu_i^\top Ns = \chi_i$; compatibility with the metric is (2) again.

Theorem 3. Step 1. By (19), $\beta \leq \alpha_{2,i}$, $\dot{\tilde{z}}_i + \beta \tilde{z}_i \geq -\zeta_i^{(\beta)}$ and $\tilde{\psi}_{1,i} \geq -[\tilde{\psi}_{1,i}]^-$; $\Pi_i^{(\beta)} + J_i e_a \geq -\tau_i$ for $i \in A$. *Step 2.* Let $d \in \text{span}\{\nu_i : i \in A\}$ have the smallest kinetic norm with $J_i d \geq -(\Pi_i^{(\beta)} + J_i e_a)$ on A ; it exists because $M^{-1}C\Delta + (k - \beta)s - e_a$ satisfies these relations, and $\|d\|_M \leq \mathfrak{d}_A[\tau]$ by Step 1 and monotonicity. The efforts $\varphi_r + \Delta^b$ with $\Delta^b = -(k - \beta)\hat{s} + C^\sharp M(e_a + d)$ satisfy the constraints of A , and Lemma 4(ii) gives, with $e_a = e_{a\parallel} + e_{a\perp}$, $P_f \leq \frac{1}{2}(k - \beta)\|s_\parallel\|_M^2 - \frac{1}{2}\langle s_\parallel, e_{a\parallel} \rangle + \frac{1}{2}\|s_\parallel\|_M(\|k - \beta\|\|s_\parallel\|_M + \|e_{a\parallel}\|_M + \|d\|_M)$. *Step 3.* Insert this into (5) and use $\|s_\perp\|_M \|e_{a\perp}\|_M + \|s_\parallel\|_M \|e_{a\parallel}\|_M \leq \|s\|_M \|e_a\|_M$; this is (21). *Step 4 (quadratic bound).* Let $\Delta = \sum_A \lambda_i H^{-1}G_i^\top$ and $d' := M^{-1}C\Delta = M^{-1}J_A^\top \lambda$; then $\|d'\|_M^2 = \sum \lambda_i J_i d'$ and $P_f = -\sum \lambda_i w_i$. Binding gives $\Pi_i^{(k)} + J_i d' = 0$ and $\Pi_i^{(k)} = \Pi_i^{(\beta)} + (k - \beta)w_i$, so by Step 1 $(\beta - k)w_i \geq J_i d' - \tau_i - J_i e_a$. Multiplying by $\lambda_i \geq 0$ and summing, $(\beta - k)P_f \leq \|d'\|_M(\mathfrak{d}_A[\tau] + \|e_a\|_M) - \|d'\|_M^2 \leq D_A^2/4$, because $\sum \lambda_i \tau_i \leq \sum \lambda_i J_i d'' = \langle d', d'' \rangle_M$ for every d'' with $J_i d'' \geq \tau_i$. *Step 5.* (i) On $E = \{t : \tilde{z}_i(t) = 0\}$, at every non-isolated point of E at which $\tilde{z}_i$ exists, $\dot{\tilde{z}}_i = 0$; isolated points are countable. (ii) is immediate. (iii) By subadditivity, $\mathfrak{d}_A[\tau] \leq \mathfrak{d}_A[\zeta + \eta]^+ + \mathfrak{d}_A[\chi]$; for independent gradients $\mathfrak{d}_A[y] \leq \min\{\|y\|_{\Lambda_A^{-1}}, \|y\|_{\Lambda_A^{-1}}^+\}$ (take $d = M^{-1}J_A^\top \Lambda_A^{-1}y$

or $d = M^{-1}J_A^\top \Lambda_A^{-1}[y]^+$; either norm can be the smaller one), and $\mathfrak{d}_A[\chi] \leq \|\chi_A\|_{\Lambda_A^{-1}} = \|\Lambda_A^{-1/2}\Gamma_A M^{-1/2}M^{1/2}s\| \leq \varrho_A\|s\|_M$. The statements for active constraints follow with $-k\|s_\perp\|_M^2 - \mu\|s_\parallel\|_M^2 + \varrho_A\|s_\parallel\|_M\|s\|_M \leq -(\mu - \varrho_A)\|s\|_M^2$, and from (22) with $D_A \leq \varrho_A\|s\|_M$ inserted into (5).

D. Proofs of Sections V and VI

Proposition 1. On I' , $u = u_r$, so $\tilde{\psi}_{1,i} = \tilde{z}_i$; both are locally absolutely continuous, hence $\dot{\tilde{z}}_i + \alpha_{2,i}\tilde{z}_i = \dot{\tilde{\psi}}_{2,i} = \dot{\tilde{\psi}}_{2,i}(\varphi) \geq 0$ a.e. on I' . From a start in $\mathcal{C}$, $\tilde{\psi}_{1,i} \geq 0$ by Lemma 2. At $s = 0$, $\hat{a}(\varphi_r) = a_r = a^{(\beta)}$ for every β , $\tilde{\psi}_{1,i} = \tilde{z}_i$ and $\chi_i = 0$, and (19) gives the value.

Theorem 4. For $\beta \geq \bar{\beta}$, $\dot{\tilde{z}}_i + \beta\tilde{z}_i \geq (\beta - \bar{\beta})\tilde{z}_i \geq 0$, so $\zeta^{(\beta)} = 0$; take $\beta = \alpha_A \geq \alpha_{\min} \geq \bar{\beta}$ in Theorem 3. (b) From a start in $\mathcal{C}$ a nominal solution keeps $\tilde{\psi}_{1,i} \geq 0$ (Lemma 2), so $\eta = 0$, and $\dot{S} \leq -k\|s_\perp\|_M^2 - \mu\|s_\parallel\|_M^2 + \varrho\|s_\parallel\|_M\|s\|_M \leq -2(\mu - \varrho)S$; for $k < \alpha_{\min}$, (22) and (5) give $\dot{S} \leq -2kS + \varrho^2\|s\|_M^2/(4(\alpha_{\min} - k))$; where $\Delta = 0$, $\dot{S} = -2kS$. So $\dot{S} \leq -2\omega S$ a.e., and $y_\epsilon := (2S + \epsilon^2)^{1/2}$ satisfies $\dot{y}_\epsilon \leq -\omega y_\epsilon + |\omega|\epsilon$; Grönwall's inequality and $\epsilon \rightarrow 0$ give (25). (c) In the same way $\dot{S} \leq -2(\mu - \varrho)S + \|s\|_M\epsilon$ and $\dot{y}_\epsilon \leq -(\mu - \varrho)y_\epsilon + |\mu - \varrho|\epsilon + \epsilon$.

Corollary 2. $s \equiv 0$ follows from (25). Then Proposition 1 with $e_a = 0$ gives $\dot{\tilde{\psi}}_{2,i}(\varphi_r) = \dot{\tilde{z}}_i + \alpha_{2,i}\tilde{z}_i \geq (\alpha_{2,i} - \bar{\beta})\tilde{z}_i \geq 0$, so φ_r satisfies all barrier constraints a.e.; since a set $A(t)$ of barrier constraints supports the correction, φ is the point of $\mathcal{X}_{A(t)}$ nearest to φ_r (Lemma 4(ii)), and $\varphi_r \in \mathcal{X}_{A(t)}$, so $\varphi = \varphi_r$ a.e. For equal second rates, sufficiency is the first part with $\bar{\beta} = \alpha_2$, and necessity is Proposition 1 with $I' = I$.

Remark 6. For each of the finitely many A , $\{t : \Lambda_A(t) \succeq \lambda I\}$ is closed and $\varrho_A \leq \|\Gamma_A M^{-1/2}\|_2/\sqrt{\lambda}$ there, with a locally bounded measurable right side; $\mathfrak{d}_{A(t)}[\chi] \leq \varrho_{A(t)}\|s\|_M$ is Step 5(iii) above. For the constant rate, as long as $\|s\|_M \leq \|s(0)\|_M$ the rate is at least the stated constant, so $\|s\|_M$ decreases.

Proposition 2. (i) u_r is the integral of a_r . (ii) Along the motion $\dot{\tilde{z}}_i = \dot{b}_i + \dot{J}_i u_r + J_i \dot{u}_r + \alpha_{1,i}\dot{h}_i$, so constraint i of (26) reads $\dot{\tilde{z}}_i + \beta\tilde{z}_i \geq 0$, and $e^{\beta t}\tilde{z}_i$ is non-decreasing. (iii) For $u_r = u$, $\tilde{z}_i = \tilde{\psi}_{1,i}$. (iv) is immediate.

Proposition 3. Strict inequalities persist under small changes of continuous data, so $\mathcal{O}$ is open. If the data $(G(p), r(p), x_0(p), Q(p))$ of a nearest-point problem depend continuously on p and the feasible set at $\bar{p}$ has a strictly feasible point x_s , the minimizer is continuous at $\bar{p}$: the minimizers near $\bar{p}$ are bounded by $\|x_s - x_0(p)\|_{Q(p)}$, a limit point $\hat{x}$ of $x^*(p_n)$ is feasible at $\bar{p}$, and comparing with the strictly feasible points $(1 - \epsilon)x^*(\bar{p}) + \epsilon x_s$, which are feasible for large n , shows that $\hat{x}$ is the unique minimizer at $\bar{p}$. Hence a_r , then φ_r , then φ are continuous on $\mathcal{O}$ (cf. [49]), and Peano's theorem and the standard continuation argument apply.

Theorem 5. Effort layer. For a command φ' let $y(\varphi') = \hat{L}a(\varphi') + \hat{L}u$ be the model value of $\hat{\ell}$. The two constraints of pair j read $\underline{y}_j \leq y_j(\varphi') \leq \bar{y}_j$ with $\underline{y}_j = -(\alpha_{1,j} + \alpha_{2,j})\dot{\ell}_j - \alpha_{1,j}\alpha_{2,j}\tilde{h}_j^-$ and $\bar{y}_j = -(\alpha_{1,j} + \alpha_{2,j})\dot{\ell}_j + \alpha_{1,j}\alpha_{2,j}\tilde{h}_j^+$, an interval of the constant length $\alpha_{1,j}\alpha_{2,j}\varpi_j$ with $\varpi_j := \bar{\ell}_j - \underline{\ell}_j - \sigma_j^- - \sigma_j^+ > 0$, because $\tilde{h}_j^- + \tilde{h}_j^+ = \varpi_j$. Since $\varphi' \mapsto y(\varphi')$ is affine and onto wherever $\hat{L}$ is invertible, the program is strictly feasible there, and at most one constraint of a pair binds. *First*

layer. In terms of $x_j = (La)_j$ the two constraints of (26) for pair j form an interval of length $\bar{\beta}(\tilde{z}_j^- + \tilde{z}_j^+) = \bar{\beta}\alpha_{1,j}\varpi_j > 0$, so (26) is strictly feasible wherever L is invertible. *Existence and invariance.* By Proposition 3 solutions exist locally; along them $(q, u) \in \mathcal{C}$ by Lemma 2 and $\tilde{z}_j^\mp \geq 0$ by Proposition 2. On $\mathcal{C}$, $-\alpha_{1,j}\tilde{h}_j^- \leq (Lu)_j \leq \alpha_{1,j}\tilde{h}_j^+$, and the same holds for Lu_r by the constraints of (7), so $q \in B$ and u, u_r are bounded: on bounded time intervals the solution stays in a compact subset of $\mathcal{O}$, so it exists for all times. *Rate.* A supporting set contains one with at most one constraint of each pair, so with independent gradients; Λ_A is a principal submatrix of $LM^{-1}L^\top$ up to signs, and the rows of Γ_A are rows of $\pm\Gamma$; hence $\varrho_A \leq \bar{\varrho}$, which is finite because $\mathcal{C}$ is compact, and Theorem 4(b) applies with $\varrho = \bar{\varrho}$.

Proposition 4. With (3), $M\dot{u} = Ma_r + Ns + Ks + C\Delta + Me_m$, and $M\dot{u}_r = Ma_r + C\Delta + Me_a^0$; subtract, and use (2) for $\dot{S}$. For (27) with $s \equiv 0$: $u = U + u_\Delta$, $\dot{s}^\circ = -\dot{u}_\Delta = ku_\Delta - M^{-1}C\Delta = -ks^\circ - M^{-1}C\Delta$, and the nominal model acceleration is $a_r = \dot{U} + ks^\circ$; for the loop of Section II with $a_r = \dot{U}$, $\dot{s} = \dot{U} - \dot{u} = -ks - M^{-1}Ns - M^{-1}C\Delta$ and the nominal model acceleration is $\dot{U} + ks + M^{-1}Ns$.

REFERENCES

- [1] A. D. Ames, X. Xu, J. W. Grizzle, and P. Tabuada, "Control barrier function based quadratic programs for safety critical systems," *IEEE Trans. Autom. Control*, vol. 62, no. 8, pp. 3861–3876, Aug. 2017.
- [2] A. D. Ames, S. Coogan, M. Egerstedt, G. Notomista, K. Sreenath, and P. Tabuada, "Control barrier functions: Theory and applications," in *Proc. 18th Eur. Control Conf. (ECC)*, 2019, pp. 3420–3431.
- [3] A. Singletary, S. Kolathaya, and A. D. Ames, "Safety-critical kinematic control of robotic systems," *IEEE Control Syst. Lett.*, vol. 6, pp. 139–144, 2022.
- [4] T. G. Molnar, R. K. Cosner, A. W. Singletary, W. Ubellacker, and A. D. Ames, "Model-free safety-critical control for robotic systems," *IEEE Robot. Autom. Lett.*, vol. 7, no. 2, pp. 944–951, Apr. 2022.
- [5] Y. Xiong, D.-H. Zhai, S. Zhang, and Y. Xia, "Multi-layered safety-critical control design for robotic systems via control barrier functions," in *Proc. 41st Chinese Control Conf. (CCC)*, 2022, pp. 3674–3679.
- [6] Q. Nguyen and K. Sreenath, "Exponential control barrier functions for enforcing high relative-degree safety-critical constraints," in *Proc. Amer. Control Conf. (ACC)*, 2016, pp. 322–328.
- [7] W. Xiao and C. Belta, "High-order control barrier functions," *IEEE Trans. Autom. Control*, vol. 67, no. 7, pp. 3655–3662, Jul. 2022.
- [8] J.-J. E. Slotine and W. Li, "On the adaptive control of robot manipulators," *Int. J. Robot. Res.*, vol. 6, no. 3, pp. 49–59, 1987.
- [9] W.-H. Zhu, Y.-G. Xi, Z.-J. Zhang, Z. Bien, and J. De Schutter, "Virtual decomposition based control for generalized high dimensional robotic systems with complicated structure," *IEEE Trans. Robot. Autom.*, vol. 13, no. 3, pp. 411–436, Jun. 1997.
- [10] W.-H. Zhu, *Virtual Decomposition Control: Toward Hyper Degrees of Freedom Robots*, ser. Springer Tracts in Advanced Robotics. Berlin, Germany: Springer, 2010, vol. 60.
- [11] J. Koivumäki, J.-P. Humaloja, L. Paunonen, W.-H. Zhu, and J. Mattila, "Subsystem-based control with modularity for strict-feedback form nonlinear systems," *IEEE Trans. Autom. Control*, vol. 68, no. 7, pp. 4336–4343, 2023.
- [12] J.-P. Humaloja, J. Koivumäki, L. Paunonen, and J. Mattila, "Decentralized observer design for virtual decomposition control," *IEEE Trans. Autom. Control*, vol. 67, no. 5, pp. 2529–2536, 2022.
- [13] G. R. Petrović and J. Mattila, "Mathematical modelling and virtual decomposition control of heavy-duty parallel-serial hydraulic manipulators," *Mech. Mach. Theory*, vol. 170, p. 104680, 2022.
- [14] M. H. Cohen, T. G. Molnar, and A. D. Ames, "Safety-critical control for autonomous systems: Control barrier functions via reduced-order models," *Annu. Rev. Control*, vol. 57, p. 100947, 2024.
- [15] M. H. Cohen, N. Csomay-Shanklin, W. D. Compton, T. G. Molnar, and A. D. Ames, "Safety-critical controller synthesis with reduced-order models," in *Proc. Amer. Control Conf. (ACC)*, 2025, pp. 5216–5221.

- [16] U. Rosolia, A. Singletary, and A. D. Ames, "Unified multirate control: From low-level actuation to high-level planning," *IEEE Trans. Autom. Control*, vol. 67, no. 12, pp. 6627–6640, Dec. 2022.
- [17] K. Garg, R. K. Cosner, U. Rosolia, A. D. Ames, and D. Panagou, "Multi-rate control design under input constraints via fixed-time barrier functions," *IEEE Control Syst. Lett.*, vol. 6, pp. 608–613, 2022.
- [18] E. Garone, S. Di Cairano, and I. Kolmanovsky, "Reference and command governors for systems with constraints: A survey on theory and applications," *Automatica*, vol. 75, pp. 306–328, Jan. 2017.
- [19] M. M. Nicotra and E. Garone, "The explicit reference governor: A general framework for the closed-form control of constrained nonlinear systems," *IEEE Control Syst. Mag.*, vol. 38, no. 4, pp. 89–107, Aug. 2018.
- [20] A. D. Ames, G. Notomista, Y. Wardi, and M. Egerstedt, "Integral control barrier functions for dynamically defined control laws," *IEEE Control Syst. Lett.*, vol. 5, no. 3, pp. 887–892, Jul. 2021.
- [21] A. J. Taylor, P. Ong, T. G. Molnar, and A. D. Ames, "Safe backstepping with control barrier functions," in *Proc. 61st IEEE Conf. Decis. Control (CDC)*, 2022, pp. 5775–5782.
- [22] Y. Wang and X. Xu, "Proxy control barrier functions: Integrating barrier-based and Lyapunov-based safety-critical control design," *Automatica*, vol. 178, p. 112364, 2025.
- [23] M. H. Cohen, E. Lavretsky, and A. D. Ames, "Compatibility of multiple control barrier functions for constrained nonlinear systems," arXiv preprint arXiv:2509.04220v1, 2025, version v1. [Online]. Available: <https://arxiv.org/abs/2509.04220v1>
- [24] W. Shaw Cortez and D. V. Dimarogonas, "Safe-by-design control for Euler–Lagrange systems," *Automatica*, vol. 146, p. 110620, 2022.
- [25] W. Xiao, C. A. Belta, and C. G. Cassandras, "Sufficient conditions for feasibility of optimal control problems using control barrier functions," *Automatica*, vol. 135, p. 109960, 2022.
- [26] A. Del Prete, "Joint position and velocity bounds in discrete-time acceleration/torque control of robot manipulators," *IEEE Robot. Autom. Lett.*, vol. 3, no. 1, pp. 281–288, 2018.
- [27] W. Shaw Cortez and D. V. Dimarogonas, "On compatibility and region of attraction for safe, stabilizing control laws," *IEEE Trans. Autom. Control*, vol. 67, no. 9, pp. 4924–4931, Sep. 2022.
- [28] M. F. Reis, A. P. Aguiar, and P. Tabuada, "Control barrier function-based quadratic programs introduce undesirable asymptotically stable equilibria," *IEEE Control Syst. Lett.*, vol. 5, no. 2, pp. 731–736, 2021.
- [29] X. Tan and D. V. Dimarogonas, "On the undesired equilibria induced by control barrier function based quadratic programs," *Automatica*, vol. 159, p. 111359, 2024.
- [30] Y. Chen, P. Mestres, J. Cortés, and E. Dall'Anese, "Independence of closed-loop equilibria and stability from the choice of control barrier function for a given safe set," *Automatica*, vol. 191, p. 113105, 2026.
- [31] F. Califano, "Passivity-preserving safety-critical control using control barrier functions," *IEEE Control Syst. Lett.*, vol. 7, pp. 1742–1747, 2023.
- [32] F. Califano, R. Zanella, A. Macchelli, and S. Stramigioli, "The effect of control barrier functions on energy transfers in controlled physical systems," arXiv preprint arXiv:2406.13420v1, 2024, version v1. [Online]. Available: <https://arxiv.org/abs/2406.13420v1>
- [33] Z. Zhang, T. Li, and N. Figueroa, "Constrained passive interaction control: Leveraging passivity and safety for robot manipulators," in *Proc. IEEE Int. Conf. Robot. Autom. (ICRA)*, 2024, pp. 13 418–13 424.
- [34] Y. Michel, M. Saveriano, and D. Lee, "A novel safety-aware energy tank formulation based on control barrier functions," *IEEE Robot. Autom. Lett.*, vol. 9, no. 6, pp. 5206–5213, 2024.
- [35] V. Kurtz, P. M. Wensing, and H. Lin, "Control barrier functions for singularity avoidance in passivity-based manipulator control," in *Proc. 60th IEEE Conf. Decis. Control (CDC)*, 2021, pp. 6125–6130.
- [36] M. Shahna, J. Kim, and J. Mattila, "RoboCompiler: Graph-native compilation of closed-chain robots for consistent modeling, control, and simulation," arXiv preprint arXiv:2609.35717v2, 2026, version v2. [Online]. Available: <https://arxiv.org/abs/2609.35717v2>
- [37] J. Carpentier, G. Saurel, G. Buondonno, J. Mirabel, F. Lamiroux, O. Stasse, and N. Mansard, "The Pinocchio C++ library: A fast and flexible implementation of rigid body dynamics algorithms and their analytical derivatives," in *Proc. IEEE/SICE Int. Symp. Syst. Integr. (SII)*, 2019, pp. 614–619.
- [38] E. Todorov, T. Erez, and Y. Tassa, "MuJoCo: A physics engine for model-based control," in *Proc. IEEE/RSJ Int. Conf. Intell. Robots Syst. (IROS)*, 2012, pp. 5026–5033.
- [39] R. Hanus, M. Kinnaert, and J.-L. Henrotte, "Conditioning technique, a general anti-windup and bumpless transfer method," *Automatica*, vol. 23, no. 6, pp. 729–739, 1987.
- [40] E. N. Johnson and A. J. Calise, "Limited authority adaptive flight control for reusable launch vehicles," *J. Guid. Control Dyn.*, vol. 26, no. 6, pp. 906–913, Nov. 2003.
- [41] F. E. Udwardia, "The general Gauss principle of least constraint," *J. Appl. Mech.*, vol. 90, no. 11, p. 111006, 2023.
- [42] S. Kolathaya and A. D. Ames, "Input-to-state safety with control barrier functions," *IEEE Control Syst. Lett.*, vol. 3, no. 1, pp. 108–113, 2019.
- [43] G. Tao, "A simple alternative to the Barbalat lemma," *IEEE Trans. Autom. Control*, vol. 42, no. 5, p. 698, 1997.
- [44] S. Galeani, S. Tarbouriech, M. Turner, and L. Zaccarian, "A tutorial on modern anti-windup design," *Eur. J. Control*, vol. 15, no. 3–4, pp. 418–440, 2009.
- [45] Robotic Systems Lab, ETH Zurich, "RSL HEAP," Software repository, commit c1b7889. [Online]. Available: https://github.com/leggedrobotics/rsl_heap
- [46] J. Breeden, K. Garg, and D. Panagou, "Control barrier functions in sampled-data systems," *IEEE Control Syst. Lett.*, vol. 6, pp. 367–372, 2022.
- [47] A. Singletary, Y. Chen, and A. D. Ames, "Control barrier functions for sampled-data systems with input delays," in *Proc. 59th IEEE Conf. Decis. Control (CDC)*, 2020, pp. 804–809.
- [48] W. Shaw Cortez, D. Oetomo, C. Manzie, and P. Choong, "Control barrier functions for mechanical systems: Theory and application to robotic grasping," *IEEE Trans. Control Syst. Technol.*, vol. 29, no. 2, pp. 530–545, Mar. 2021.
- [49] P. Mestres, A. Allibhoy, and J. Cortés, "Regularity properties of optimization-based controllers," *Eur. J. Control*, vol. 81, p. 101098, Jan. 2025.



Mehdi Heydari Shahna received the D.Sc. (Tech.) degree with distinction in Automation Science and Engineering from Tampere University, Finland, in 2025. He is currently a postdoctoral researcher at Tampere University. His research interests include physical AI, robot learning, safe control, and robust control.



Jouni Mattila received a Ph.D. in automation engineering from Tampere University of Technology, Tampere, Finland, in 2000. He is currently a professor of machine automation with the Unit of Automation Technology and Mechanical Engineering at Tampere University. His research interests include machine automation, nonlinear-model-based control of robotic manipulators, and energy-efficient control of heavy-duty mobile manipulators.