KFX Continuous Mathematical Model: Non-Bypassability via Differential Inclusions, Viability, and Invariance

Kaifan XIE
(0009-0005-6911-7295)

February 8, 2026

Abstract

This document gives a purely mathematical continuous-time model in which a distinguished *anchor state* cannot be bypassed for a class of *high-impact controls*. "Non-bypassability" is formalised as an invariance/unreachability property of a *state–control constraint set*. The core enforcement is written in an "originally continuous" form using *differential inclusions* (set-valued dynamics), *viability theory*, and (optionally) *projected / sweeping processes*. No implementation narrative is used; only dynamical systems, constraints, and proofs.

Contents

1 Mathematical Problem Statement

1.1 Goal (non-bypassability)

Let $u(t)$ be the control input applied to the actuators. Define a subset of controls $\mathcal{U}_{\mathrm{HI}}(z) \subseteq \mathcal{U}$ as *high-impact* at state z. The objective is to construct a closed-loop system such that:

> No admissible trajectory can realise a high-impact control value without satisfying an anchor-gating condition.

1.2 How this will be done (purely mathematical)

We will:

- define a *forbidden set* in (z, u) space corresponding to bypass events;
- define an *admissible constraint set* $\mathcal{K}$ in (z, u) space;
- enforce $\mathcal{K}$ by a *differential inclusion* (viability / invariance);
- provide equivalences with projection and QP enforcement.

2 Time, State, Control, and Disturbance

2.1 Time

Time $t \in [0, \infty)$. When hybrid transitions are present, event times are a strictly increasing sequence $\{t_k\}_{k\in\mathbb{N}}$ with no Zeno accumulation unless stated.

2.2 State space

Let the total state be

$$x(t) \in \mathcal{X} \subseteq \mathbb{R}^n.$$

Introduce an *anchor state* $a(t) \in \mathcal{A} \subseteq \mathbb{R}^{n_a}$ and define the full state

$$z(t) := \begin{bmatrix} x(t) \\ a(t) \end{bmatrix} \in \mathcal{Z} \subseteq \mathbb{R}^{n+n_a}.$$

2.3 Control input

$$u(t) \in \mathcal{U} \subseteq \mathbb{R}^m.$$

2.4 Disturbance / adversary input

$$d(t) \in \mathcal{D} \subseteq \mathbb{R}^p.$$

No probabilistic assumptions are required; boundedness may be assumed.

2.5 Measurability

Assume $u(\cdot)$ and $d(\cdot)$ are measurable and essentially bounded on finite horizons.

3 Dynamics: From ODE to Differential Inclusion

3.1 Nominal (single-valued) flow dynamics

Start with a Carathéodory control system

$$\dot{z}(t) = F\big(z(t), u(t), d(t)\big) \quad \text{for a.e. } t. \tag{1}$$

3.2 Set-valued dynamics (core of "continuous enforcement")

To encode hard constraints without discrete if/else narration, we move to a differential inclusion:

$$\dot{z}(t) \in \mathcal{F}\big(z(t)\big) \quad \text{for a.e. } t, \tag{2}$$

where $\mathcal{F} : \mathcal{Z} \rightrightarrows \mathbb{R}^{n+n_a}$ is set-valued.

The most direct form is to make the control an *implicit selection*:

$$\dot{z}(t) \in \Big\{F\big(z(t), u, d(t)\big) : u \in \mathcal{U}_{\text{adm}}(z(t))\Big\}. \tag{3}$$

The entire non-bypass property reduces to defining $\mathcal{U}_{\text{adm}}(z)$ so that bypass actions are *not selectable*.

Assumption 3.1 (Nonemptiness)**.** For all $z \in \mathcal{Z}$, the admissible control set $\mathcal{U}_{\text{adm}}(z)$ is nonempty.

Assumption 3.2 (Regularity for existence)**.** Assume $\mathcal{U}_{\text{adm}}(z)$ is measurable in t through $z(t)$, and $F(\cdot, u, \cdot)$ is locally Lipschitz in z for each fixed u, and $\mathcal{U}_{\text{adm}}(\cdot)$ is upper hemicontinuous with compact values. Then (3) admits absolutely continuous solutions on finite horizons.

4 High-Impact Set as Inequalities (No Narrative)

4.1 Impact function and threshold

Define an impact function

$$I : \mathcal{Z} \times \mathcal{U} \to \mathbb{R},$$

and a threshold $\tau \in \mathbb{R}$. High-impact controls are exactly:

$$\mathcal{U}_{\text{HI}}(z) = \{u \in \mathcal{U} : I(z, u) \geq \tau\}. \tag{4}$$

4.2 Safe set (complement or conservative subset)

Define a safe set map $\mathcal{U}_{\text{SAFE}}(z) \subseteq \mathcal{U}$ such that

$$\mathcal{U}_{\text{SAFE}}(z) \cap \mathcal{U}_{\text{HI}}(z) = \varnothing. \tag{5}$$

Remark 4.1. (5) is the only structural requirement used later; $\mathcal{U}_{\text{SAFE}}(z)$ can be any conservative "low-impact" control family.

5 Anchor-Gating as Pure State Constraints

5.1 Gated subset via inequalities

Represent the gated subset as:

$$\mathcal{Z}_g = \{z \in \mathcal{Z} : h_i(z) \geq 0, \ i = 1, \ldots, r\}, \tag{6}$$

where $h_i : \mathcal{Z} \to \mathbb{R}$ are (at least) locally Lipschitz, and typically C^1. The key is that h_i depend on the anchor component a (since $z = [x; a]$).

5.2 Binary gating predicate (optional)

You may also define

$$g(z) = \mathbf{1}\{z \in \mathcal{Z}_g\}.$$

But the inequalities (6) are the real object; g is just shorthand.

6 Non-Bypassability as a Constraint Set in (z, u) Space

6.1 Forbidden set

Define the forbidden bypass set:

$$\mathcal{F} := \{(z, u) \in \mathcal{Z} \times \mathcal{U} : \; I(z, u) \geq \tau \; \wedge \; z \notin \mathcal{Z}_g\}. \tag{7}$$

6.2 Admissible set (graph constraint)

Define the admissible set:

$$\mathcal{K} := \{(z, u) \in \mathcal{Z} \times \mathcal{U} : \; z \notin \mathcal{Z}_g \Rightarrow I(z, u) < \tau\}. \tag{8}$$

Equivalently (no implication symbol):

$$\mathcal{K} = \Big(\{(z, u) : z \in \mathcal{Z}_g\} \cap (\mathcal{Z} \times \mathcal{U})\Big) \; \cup \; \Big(\{(z, u) : z \notin \mathcal{Z}_g\} \cap \{(z, u) : I(z, u) < \tau\}\Big). \tag{9}$$

Proposition 6.1 (Non-bypassability is $\mathcal{F}$-unreachability / $\mathcal{K}$-viability)**.** A closed-loop trajectory is non-bypassable iff $(z(t), u(t)) \notin \mathcal{F}$ for all t (a.e.), equivalently $(z(t), u(t)) \in \mathcal{K}$ for all t (a.e.).

7 Admissible Control Map and Differential Inclusion (Main Construction)

7.1 Admissible control map

Define the admissible control set map:

$$\mathcal{U}_{\text{adm}}(z) := \begin{cases} \mathcal{U}, & z \in \mathcal{Z}_g, \\ \mathcal{U} \setminus \mathcal{U}_{\text{HI}}(z), & z \notin \mathcal{Z}_g. \end{cases} \tag{10}$$

Using (4), the second line is:

$$\mathcal{U}_{\text{adm}}(z) = \{u \in \mathcal{U} : I(z, u) < \tau\} \quad \text{when } z \notin \mathcal{Z}_g.$$

7.2 Enforced dynamics as a differential inclusion

The core enforced model is:

$$\dot{z}(t) \in \Big\{F\big(z(t), u, d(t)\big) : u \in \mathcal{U}_{\text{adm}}(z(t))\Big\} \quad \text{for a.e. } t. \tag{11}$$

Theorem 7.1 (Non-bypassability by construction (pure DI form))**.** Any solution $(z(\cdot), u(\cdot))$ of (11) satisfies

$$z(t) \notin \mathcal{Z}_g \;\; \Rightarrow \;\; I(z(t), u(t)) < \tau \quad \text{for a.e. } t.$$

Equivalently, $(z(t), u(t)) \notin \mathcal{F}$ for a.e. t.

Proof. If $z(t) \notin \mathcal{Z}_g$, then by definition (10), $u(t) \in \mathcal{U}_{\text{adm}}(z(t))$ implies $I(z(t), u(t)) < \tau$. Therefore $(z(t), u(t)) \notin \mathcal{F}$ a.e. □

Remark 7.1. This theorem contains the entire "cannot bypass the anchor" statement without any external semantics: the bypass pair set $\mathcal{F}$ is simply excluded from the admissible graph.

8 Equivalent Enforcements: Projection, QP, and Complementarity

8.1 Nominal proposal and metric projection (selection operator)

Let a nominal proposal be $\hat{u}(t) = \mu(z(t))$ (arbitrary). Define a realised selection as:

$$u(t) \in \Pi_{\mathcal{U}_{\mathrm{adm}}(z(t))}\big(\hat{u}(t)\big), \tag{12}$$

where $\Pi_{\mathcal{S}}(v) := \arg\min_{w\in\mathcal{S}} \|w - v\|^2$ (set-valued if minimiser not unique).

Then the closed-loop system is the differential inclusion:

$$\dot{z}(t) = F\big(z(t), u(t), d(t)\big), \quad u(t) \in \Pi_{\mathcal{U}_{\mathrm{adm}}(z(t))}(\mu(z(t))). \tag{13}$$

8.2 QP enforcement (convex case)

If $\mathcal{U}$ is convex and $I(z, u) < \tau$ defines a convex constraint in u for each fixed z (e.g., I convex in u), then when $z \notin \mathcal{Z}_g$ the selection can be written as:

$$u(t) = \arg\min_{u\in\mathcal{U}} \|u - \hat{u}(t)\|^2 \quad \text{s.t.} \quad I(z(t), u) \leq \tau - \epsilon, \tag{14}$$

for a margin $\epsilon \geq 0$ (strict $<$ replaced by $\leq$ with margin).

8.3 Complementarity (switching surface) form

Introduce a nonnegative slack variable $\lambda(t) \geq 0$ and define:

$$\phi(z) := \min_{i=1,\ldots,r} h_i(z),$$

so that $z \in \mathcal{Z}_g$ iff $\phi(z) \geq 0$. Define a mode inequality:

$$\phi(z(t)) < 0 \Rightarrow I(z(t), u(t)) \leq \tau - \epsilon.$$

This can be encoded by complementarity (one of the constraints must be active):

$$\lambda(t) \geq 0, \quad (\tau - \epsilon - I(z(t), u(t))) \geq 0, \quad \lambda(t)\,(\tau - \epsilon - I(z(t), u(t))) = 0 \tag{15}$$

whenever $\phi(z(t)) < 0$, and $\lambda(t) = 0$ whenever $\phi(z(t)) \geq 0$. This gives a continuous-time KKT-like enforcement view.

9 Viability / Invariance in State Space (Optional Strengthening)

Up to now, non-bypassability is enforced by restricting (z, u) pairs. A stronger property is to ensure certain state sets are forward invariant under admissible controls.

9.1 Tangent cone condition (viability)

Let $\mathcal{S} \subseteq \mathcal{Z}$ be closed. The Bouligand tangent cone at $z \in \mathcal{S}$ is denoted $\mathcal{T}_{\mathcal{S}}(z)$. A standard viability sufficient condition is:

$$\exists u \in \mathcal{U}_{\mathrm{adm}}(z) \text{ such that } F(z, u, d) \in \mathcal{T}_{\mathcal{S}}(z) \quad \forall d \in \mathcal{D}$$

for all $z \in \mathcal{S}$. This ensures there exist trajectories that remain in $\mathcal{S}$ (viability), or under stronger conditions, all trajectories remain (invariance).

9.2 Barrier-function sufficient condition (classical)

If $\mathcal{S} = \{z : h(z) \geq 0\}$ with C^1 function h, a sufficient condition for forward invariance is:

$$\sup_{u \in \mathcal{U}_{\mathrm{adm}}(z)} \inf_{d \in \mathcal{D}} \nabla h(z)^\top F(z, u, d) \;\geq\; -\alpha(h(z)),$$

for an extended class-$\mathcal{K}$ function α.

Remark 9.1. This is independent of non-bypassability enforcement; it is used when you additionally want to constrain $z(t)$ to remain inside some region.

10 Projected Dynamics / Sweeping Process (Hard State Constraints on $\mathcal{Z}_g$)

This section is the "originally continuous" alternative where the *state itself* is hard-constrained to a set and the dynamics is projected. Use this if you want the system to *physically prevent leaving* a set, rather than only gating actions outside it.

10.1 Hard state constraint set

Let $\mathcal{C} \subseteq \mathcal{Z}$ be a closed convex set (e.g., $\mathcal{C} = \mathcal{Z}_g$ or a subset). Define the normal cone $\mathcal{N}_{\mathcal{C}}(z)$.

10.2 Moreau sweeping / projected differential inclusion

A standard form is:

$$\dot{z}(t) \in F\big(z(t), u(t), d(t)\big) \;-\; \mathcal{N}_{\mathcal{C}}(z(t)), \quad z(t) \in \mathcal{C}. \tag{16}$$

Intuition (pure geometry): when the flow tries to exit $\mathcal{C}$, the normal cone term supplies the minimal "reaction" to keep $z(t)$ in $\mathcal{C}$.

10.3 Connecting to non-bypassability

If you set $\mathcal{C}$ to encode "anchor-present" states, then bypassing is made geometrically impossible by invariance of $\mathcal{C}$. However, the earlier approach (11) is typically the exact match to "high-impact requires gating" without forcing $z \in \mathcal{Z}_g$ always.

11 Hybrid Extension (Optional but Included)

11.1 Jump set and jump map

To include discrete events, define a jump set $\mathcal{J} \subseteq \mathcal{Z}$ and a set-valued jump map

$$z^+ \in G(z) \subseteq \mathcal{Z} \quad \text{for } z \in \mathcal{J}.$$

A hybrid execution alternates between flows (11) (or (13), (16)) and jumps on $\mathcal{J}$.

11.2 No-Zeno assumption (if needed)

Assumption 11.1 (No Zeno behaviour)**.** Hybrid executions do not exhibit infinitely many jumps in finite time.

11.3 Jump consistency with non-bypassability

A sufficient condition for preserving non-bypassability across jumps is:

$$(z,u) \in \mathcal{K} \ \wedge \ z^+ \in G(z) \ \Rightarrow \ \exists u^+ \in \mathcal{U}_{\mathrm{adm}}(z^+).$$

In other words, jumps cannot "teleport" the system into a state where admissible controls are empty.

12 Responsibility Allocation (Optional Pure Mathematics)

This section is optional and orthogonal: it is a continuous state on a simplex coupled to the main dynamics.

12.1 Simplex state

Let $\rho(t) \in \Delta^{N-1}$, i.e.

$$\rho_i(t) \geq 0, \quad \sum_{i=1}^{N} \rho_i(t) = 1.$$

12.2 Dynamics

Let $c_i(t) \geq 0$ be measurable contribution signals, and define

$$\tilde{c}_i(t) = \frac{c_i(t)}{\sum_{j=1}^{N} c_j(t) + \varepsilon_0}, \quad \varepsilon_0 > 0,$$

$$\dot{\rho}_i(t) = \gamma(\tilde{c}_i(t) - \rho_i(t)), \quad \gamma > 0.$$

12.3 Coupling constraint (anchor share during high impact)

If the anchor index is A, enforce:

$$I(z(t), u(t)) \geq \tau \Rightarrow \rho_A(t) \geq \kappa_{\min}.$$

This is simply another constraint set in the extended space (z, u, ρ).

13 Main Theorem (Unified Continuous Mathematics Form)

Theorem 13.1 (Non-bypassability as unreachability under a differential inclusion)**.** Let high-impact controls be defined by (4), and gated states by (6). Let admissible controls be (10), and let $(z(\cdot), u(\cdot))$ satisfy the enforced inclusion (11). Then the forbidden bypass set (7) is unreachable:

$$(z(t), u(t)) \notin \mathcal{F} \quad \text{for a.e. } t \geq 0.$$

Equivalently, $(z(t), u(t)) \in \mathcal{K}$ for a.e. t with $\mathcal{K}$ given by (8).

Proof. By (11), $u(t) \in \mathcal{U}_{\mathrm{adm}}(z(t))$ a.e. If $z(t) \notin \mathcal{Z}_g$, then by (10) we must have $I(z(t), u(t)) < \tau$, hence $(z(t), u(t)) \notin \mathcal{F}$. If $z(t) \in \mathcal{Z}_g$, then $(z(t), u(t))$ cannot belong to $\mathcal{F}$ by the definition of $\mathcal{F}$. Therefore $\mathcal{F}$ is unreachable. $\square$

14 Completeness Checklist (Minimal Objects, Pure Maths)

- Spaces $\mathcal{X}, \mathcal{A}, \mathcal{Z}$ and disturbance set $\mathcal{D}$.
- Nominal single-valued dynamics $F(z, u, d)$.
- Impact function $I(z, u)$ and threshold τ defining $\mathcal{U}_{\mathrm{HI}}(z)$.
- Gated set $\mathcal{Z}_g$ via inequalities $h_i(z) \geq 0$ (anchor enters through $z = [x; a]$).
- Admissible control map $\mathcal{U}_{\mathrm{adm}}(z)$, defining the enforced inclusion (11).
- (Optional) a selection operator: projection (12) or QP (14).
- (Optional) viability / barrier conditions for additional state invariance.
- (Optional) sweeping process (16) if hard state constraints are required.

15 Appendix: Connections Between the Forms

15.1 From DI to projection/QP

Given $\hat{u} = \mu(z)$, any measurable selection $u \in \Pi_{\mathcal{U}_{\mathrm{adm}}(z)}(\hat{u})$ yields a solution of the inclusion (11). Conversely, if $u(t) \in \mathcal{U}_{\mathrm{adm}}(z(t))$, it can be seen as the solution of a QP with appropriate objective and constraints (convex case).

15.2 Why this is "continuous mathematics unified"

The model is unified because:

- "Policy" appears as set-valued admissibility $\mathcal{U}_{\mathrm{adm}}(z)$ (a geometric object);
- Enforcement is a differential inclusion (11) (continuous-time object);
- Non-bypassability is unreachability of $\mathcal{F}$ (reachability object) and viability of $\mathcal{K}$ (invariance object);
- Optional hard state constraints use a normal cone (sweeping process), also continuous-time.