Verification of Neural Network Controllers: Inverted Pendulum Benchmark and Extension to Tethered Delivery

Calum A

16/9/2025

1 Overview & Scope

This coursework project explores the safe control of autonomous systems with neural network (NN) components. I propose to begin with the inverted pendulum benchmark outlined in the ARCH-COMP document, then extend the same verification workflow to a novel cyber-physical system: drone winched delivery.

Aerial winched delivery - pioneered by companies like Zipline[1] - uses an UAV (drone) to lower packages on a tether via a motorised winch. While efficient, this introduces risks such as payload swing, slack or broken tether, winch overload, and collisions with the environment.

To study this, we model a stationary UAV acting as an anchor point, with the plant consisting of the winch, tether, and payload. The controller commands winch rate to follow a descent profile while suppressing swing under wind disturbances. We then verify both NN properties (e.g. bounded outputs, robustness) and closed-loop safety of the overall system over a finite horizon.

2 Approach

Phase A: Inverted Pendulum Benchmark

We first reproduce the classical inverted pendulum benchmark used in ARCH-COMP:

[1] www.zipline.com/technology

- Dynamics: pendulum of mass m and length L, actuated by torque T, with viscous friction c.
- Equations:
$$\ddot{\theta} = \frac{g}{L}\sin\theta + \frac{1}{mL^2}T - c\dot{\theta},$$
where θ is the angle relative to the upward vertical.
- State-space form: $x_1 = \theta,\ x_2 = \dot{\theta}$,
$$\dot{x}_1 = x_2, \quad \dot{x}_2 = \frac{g}{L}\sin x_1 + \frac{1}{mL^2}(T - cx_2).$$
- Controllers trained using behaviour cloning.
- Typical parameters: $m = 0.5, L = 0.5, c = 0, g = 1, \Delta t = 0.05$.
- Initial set: $x \in [1.0, 1.2] \times [0.0, 0.2]$.
- Specification: $\forall t \in [0.5, 1] : \theta \in [0, 1]$.

This system provides a minimal but non-trivial case for:

- NN property verification (bounded output, robustness, monotonicity) using tools such as Vehicle/Marabou.
- Closed-loop reachability analysis using CORA, to check angle envelopes and actuation safety.

Phase B: Extension to Tethered Delivery

Having validated the workflow on the inverted pendulum, we extend the same verification pipeline to a winched payload (tethered delivery) system:

- Plant: stationary UAV (anchor point) + winch + tether + payload.
- States: $x = [L,\ \dot{L},\ \phi,\ \dot{\phi}]^\top$, where L is tether length and ϕ swing angle.
- Dynamics: variable-length pendulum, with actuator model $\dot{L} = u$ or $\tau_w\ddot{L} + \dot{L} = u$.
- Safety properties: bounded swing angle, no slack/overload in tension, safe tracking of descent profile.
- Verification: NN-level properties in Vehicle/Marabou; closed-loop reachability in CORA over finite horizon.

This two-phase approach balances tractability with novelty: we first obtain reproducible results on a known benchmark, then demonstrate how the same methods transfer to a safety-critical real-world inspired system.

3 Assumptions (Tethered Delivery)

- Anchor point fixed in space (UAV holds position).
- Planar motion in vertical plane; small-angle linearisation used for verification.
- Bounded lateral disturbance $a_w(t)$ (wind proxy).
- Inputs/outputs normalised for NN training and verification.
- Winch tracks commanded rate within limits.

4 States, Inputs, Outputs (Tethered Delivery)

States:

$$x = [L,\ \dot{L},\ \phi,\ \dot{\phi}]^\top$$

- L (m): tether length
- $\dot{L}$ (m/s): tether length rate
- ϕ (rad): swing angle (0 = vertical down)
- $\dot{\phi}$ (rad/s): angular rate

Input (control): u, winch rate command (m/s), after governor: $|u| \le u_{\max}$. i.e. actual input seen by the winch is not the raw neural network output, but the corrected version that has passed through a governor layer.

Disturbance: $a_w(t)$ (m/s^2), lateral acceleration proxy, $|a_w| \le a_{\max}$.

Outputs of interest:

- Tether tension T (N)
- Pod position $x = L\sin\phi,\ z = L\cos\phi$

5 Dynamics

Viscous terms: c_ϕ (about pivot), c_L (line); mass m, gravity g.

Angular Equation of Motion[2]

$$L\ddot{\phi} + 2\dot{L}\dot{\phi} + \frac{c_\phi}{mL}\dot{\phi} + g\sin\phi = a_w(t)\cos\phi$$

Length / tension relation

$$\ddot{L} - L\dot{\phi}^2 + \frac{c_L}{m}\dot{L} - g\cos\phi = -\frac{T}{m} + a_w(t)\sin phi$$

$$\Rightarrow \quad T = m\left(-\ddot{L} + L\dot{\phi}^2 + g\cos\phi - a_w(t)\sin\phi\right) - c_L\dot{L}$$

Actuator model (choose for verification)

- Kinematic winch (simplest): $\dot{L} = u$ (rate-limited & saturated).
- First-order (optional): $\tau_w\ddot{L} + \dot{L} = u$.

Small-angle linearisation

Assuming small angles we can linearise the equation of motion to make it friendlier for verification.

$$\sin\phi \approx \phi,\ \cos\phi \approx 1 \quad \Rightarrow \quad L\ddot{\phi} + 2\dot{L}\dot{\phi} + \frac{c_\phi}{m}\dot{\phi} + g\phi = a_w(t)$$

6 Controller Stack

- NN policy f_θ: tiny multilayer perceptron (MLP), inputs $[\phi, \dot{\phi}, L, \dot{L}]$ (normalised), output $u_{\text{NN}} \in [-u_{\max}, u_{\max}]$.
- Command governor: saturate/rate-limit; blend with baseline swing-damping u_{PID} if desired; track $L_{\text{ref}}(t)$.
- Runtime assurance (shield): override/clip to maintain $T \in [T_{\min}, T_{\max}]$, $|\phi| \leq \phi_{\max}$, $|u| \leq u_{\max}$.

7 Operating Ranges (example numbers)

- $m = 2.0$ kg, $g = 9.81$
- $c_\phi = 0.3$ N·m·s, $c_L = 5$ N·s/m

[2] I derived the equations of motion below using the Euler-Lagrange approach, v happy for someone to sense check my work!!

- $u_{\max} = 0.6$ m/s, $|\dot{u}| \leq 1.0$ m/s^2
- $T_{\min} = 5$ N (no slack), $T_{\max} = 400$ N
- $\phi_{\max} = 10^\circ \approx 0.1745$ rad
- Disturbance $a_w \in [-0.5, 0.5]$ m/s^2
- Descent profile $L_{\text{ref}}(t)$: $10 \to 12$ m over 8 s (0.25 m/s nominal)

8 Initial & Disturbance Sets (for CORA)

$$\mathcal{X}_0 : \; L \in [10, 12] \text{ m}, \; \dot{L} = 0, \; \phi \in [-5^\circ, 5^\circ], \; \dot{\phi} \in [-5^\circ/\text{s}, 5^\circ/\text{s}]$$

$a_w(t)$ piecewise-constant per step within bounds.

9 Verification Properties

A) Stand-alone NN (Vehicle/Marabou)

- Bounded output: $\forall x \in \mathcal{X} : \; u_{\min} \leq f_\theta(x) \leq u_{\max}$.
- Robustness (ϵ-ball): $\forall x^*, \forall x : \; \|x - x^*\|_\infty \leq \epsilon \Rightarrow |f_\theta(x) - f_\theta(x^*)| \leq \delta$. Or Lipschitz: $|f_\theta(x) - f_\theta(x^*)| \leq L\|x - x^*\|_\infty$.
- Anti-slack rule: if $T(x) \leq T_{\text{low}}$ and $|\phi| \geq \phi_g$, then $f_\theta(x) \leq 0$ (no payout).
- Rate moderation (optional): if $|\phi|$ increases then $|f_\theta(x)|$ does not increase beyond a bound.

B) Closed-loop CPS (CORA, finite horizon $T_h = 5$–10 s)

- Swing envelope: $|\phi(t)| \leq \phi_{\max}$ for all $t \in [0, T_h]$.
- No slack / overload: $T_{\min} \leq T(t) \leq T_{\max}$.
- Profile tracking: $|L(t) - L_{\text{ref}}(t)| \leq \Delta L_{\max}$ (e.g., 0.5 m).
- Horizontal corridor: $|x(t)| = |L \sin \phi| \leq x_{\max}$ (e.g., 1.0 m).
- Ground clearance: $z(t) = -L \cos \phi \geq z_{\min}$ until touchdown.