Autonomous Highway Overtaking with Reduced Lane Widths

Reproduction of the Collision Metric $C(t)$ and STPA Safety Analysis

Tahar Herri

McMaster University
CAS 781 — Computer & Software Engineering

December 18, 2025

Outline

1. Problem and scenario
2. **Part I** — Collision metric $C(t)$: definition, analysis, reproduction
3. Why, in reality, $C(t)$ is essentially invariant to lane width w (under Side VB, $S = w/2$)
4. **Part II** — STPA: Steps 1–3 + fault injection
5. Conclusions

Why reduced lane widths?

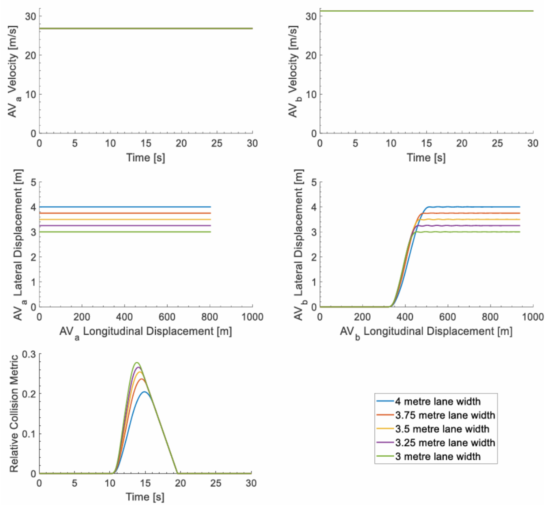
- Motivation: AVs may track lanes more precisely $\Rightarrow$ lanes could be narrower to improve capacity.
- Risk: smaller margins during critical maneuvers (here: **overtaking**).
- Setup: two AVs on a two-lane highway:
  - AVa: lead vehicle
  - AVb: overtaking vehicle

Lane widths tested:
$w \in \{4.0, 3.75, 3.5, 3.25, 3.0\}$ m.

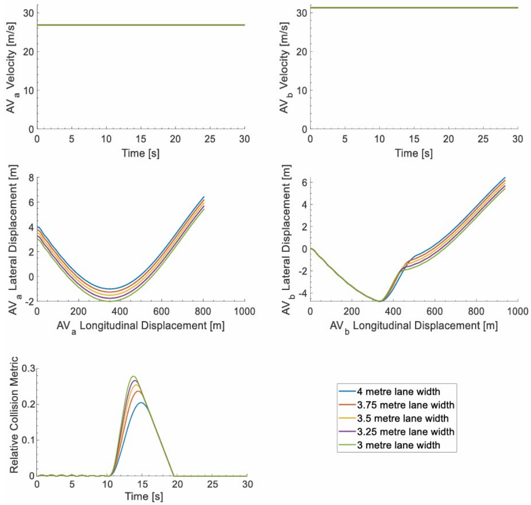
This project

- Reproduce the paper's VB-based metric $C(t)$
- Straight and curved road sections
- STPA + representative unsafe-control injection

Reference paper figures (Straight vs Curved)



Paper: Straight highway



Paper: Curved highway

Virtual Boundaries (VBs) and collision metric $C(t)$

Relative separations

$$y_s(t) = y_b(t) - y_a(t)$$
$$x_s(t) = x_b(t) - x_a(t)$$

Collision metric (clamped)

$$C(t) = \left[1 - \frac{|x_s(t)|}{U_{af}(v_a) + U_{br}(v_b)}\right]^+ \left[1 - \frac{|y_s(t)|}{S_{bl} + S_{ar}}\right]^+$$

$[z]^+ := \max(0, \min(1, z))$

Key paper assumption

Side VBs scale with lane width:

$$S_{nl} = S_{nr} = \frac{w}{2} \quad \Rightarrow \quad S_{bl} + S_{ar} = w$$

Important

w only enters the **lateral normalization** term via $(S_{bl} + S_{ar})$.

Why $C(t)$ should be independent of lane width w

Straight scenario with lane-center tracking:

$$y_a(t) = w, \qquad y_b(t) = f(t)\, w, \quad f(t) \in [0, 1]$$

$$y_s(t) = y_b(t) - y_a(t) = (f(t) - 1)\, w$$

Lateral factor cancels w exactly

Using $S_{bl} + S_{ar} = w$:

$$\gamma_{\text{lat}}(t, w) = 1 - \frac{|y_s(t)|}{S_{bl} + S_{ar}} = 1 - \frac{|(f(t) - 1)\, w|}{w}$$
$$= 1 - |f(t) - 1| \quad \textbf{(no } w\textbf{)}$$

Longitudinal factor (no explicit w)

$$\gamma_{\text{long}}(t) = 1 - \frac{|x_s(t)|}{U_{af}(v_a(t)) + U_{br}(v_b(t))}$$

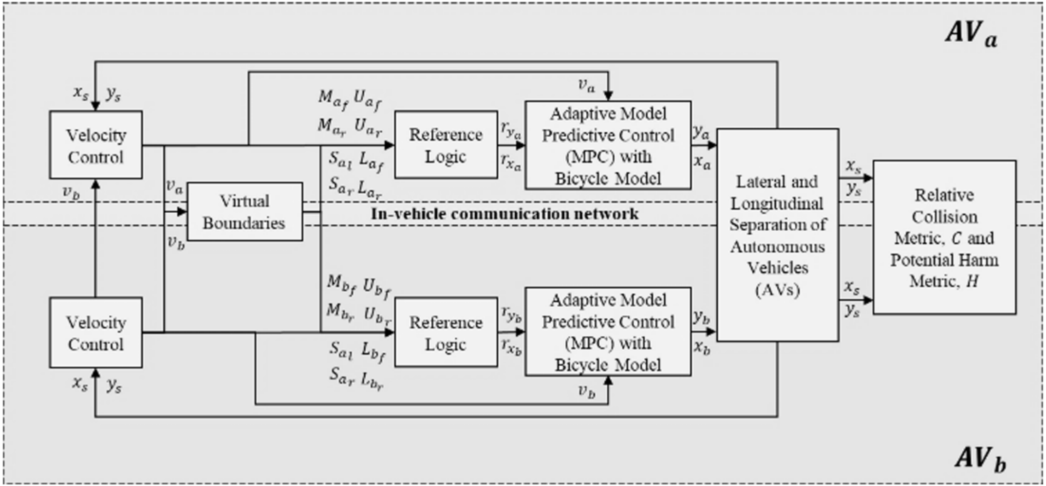
Combined metric

$$C(t, w) = \gamma_{\text{long}}(t)\, \gamma_{\text{lat}}(t, w) = \gamma_{\text{long}}(t)\, \left[1 - |f(t) - 1|\right]$$

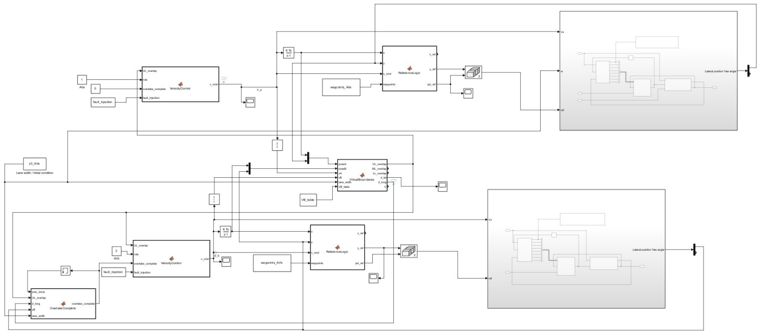
Takeaway

The lane width w cancels out **exactly** in the lateral term. Thus, under the side-VB definition $S_{nl} = w/2$ and lane-centre trajectories, the lateral contribution to C is **mathematically independent of** w. Therefore, if the model follows the paper's geometry and VB definitions, $C(t)$ should be practically the same for all w.

Simulation Model from the paper



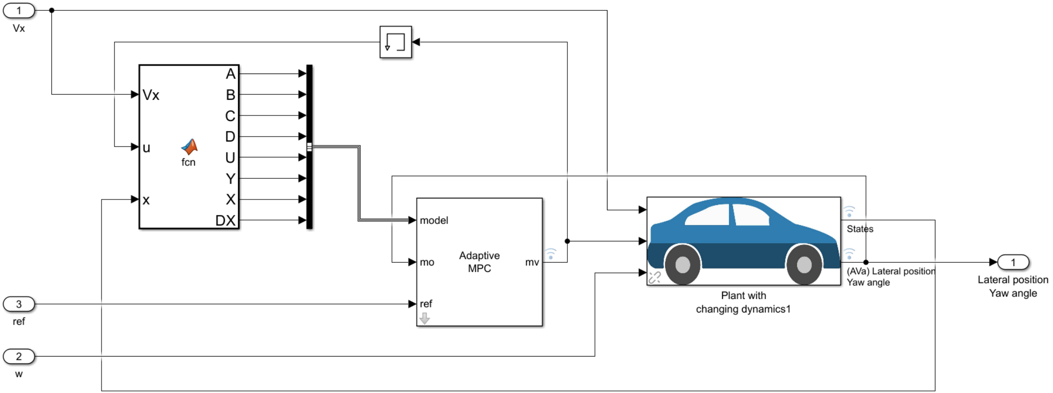
Simulink implementation (single model, all w)



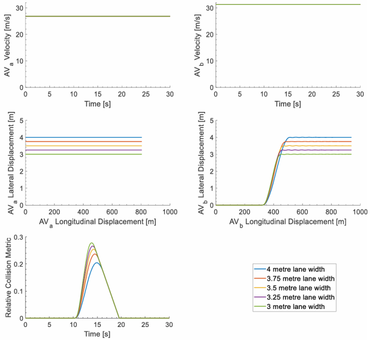
Global model: VB overlap + $C(t)$ + DR speed logic

- Same architecture for straight and curved scenarios
- Lateral path via waypoints (per w)
- `VelocityControl`: Deontological Rules (DRs) for v_a and v_b
- `VirtualBoundaries`: overlap checks + $C(t)$ computation

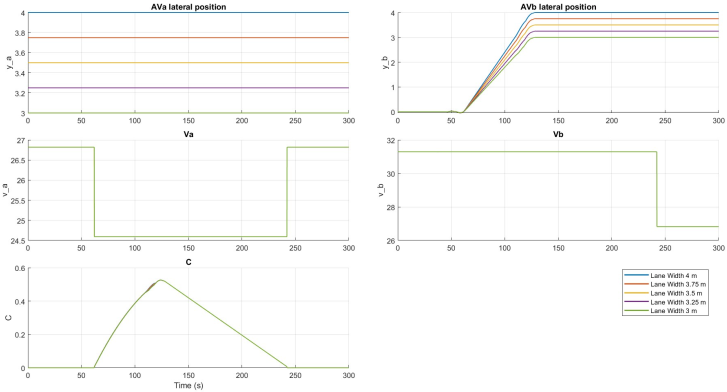
MPC subsystem (both vehicles)



Results — Straight: paper vs reproduction

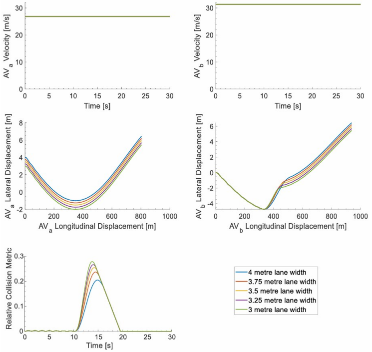


Paper: $C_{\max}$ increases as w decreases

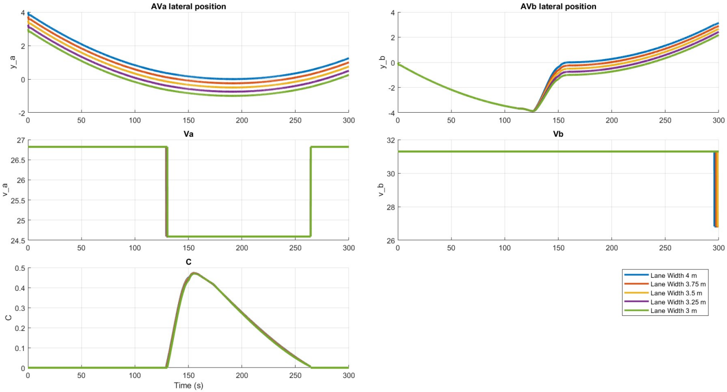


Reproduction: $C(t)$ curves overlap (weak/no w effect)

Results — Curved: paper vs reproduction



Paper: $C_{\max}$ increases as w decreases



Reproduction: $C(t)$ curves overlap (weak/no w effect)

Part I — Key conclusions

- With $S_{nl} = S_{nr} = w/2$ and lane-center tracking, the **lateral term is w-invariant**.
- Our Simulink implementation follows the stated method $\Rightarrow C(t)$ nearly identical across w.
- The paper's stronger trend likely requires **additional, undocumented modeling choices** (offsets, vehicle geometry, fixed margins, different VB logic, etc.).

STPA: objective and scope

Objective

Identify unsafe control situations amplified by reduced lane width (w), and convert them into **actionable safety constraints** and **simulation test cases**.

Scope (where unsafe control can emerge)

- **Decision layer:** when to overtake / abort, and how VB limits gate the maneuver
- **Execution layer:** tracking the lane-change (lateral MPC) + headway/speed management (longitudinal logic)
- **Feedback layer:** what the controller believes about the world (lane width, lane center, AVa/AVb relative state)

Outputs of the STPA

- Losses & Hazards
- Unsafe Control Actions (UCAs)
- Safety constraints (controller-level)
- One UCA tested via simulation fault injection

Step 1 — System boundary, losses, hazards

System boundary (in scope)

- **Decision & safety layer:** overtake planner + Virtual Boundaries (VBs)
- **Control layer:** lateral MPC + longitudinal speed control
- **Perception/estimation:** vehicle pose, lane width, lane center, relative states
- **Execution & comms:** V2V messages, actuators, vehicle dynamics

Environment (out of scope)

Traffic rules, road marking quality, other traffic, weather/surface.

Losses (L)

ID	Loss
L1	Collision AVa–AVb
L2	Collision with infrastructure/roadside objects
L3	Severe emergency maneuver
L4	Violation of VB-based ethical rules

Hazards (H)

ID	Hazard
H1	Insufficient **lateral** separation
H2	Insufficient **longitudinal** separation
H3	Incorrect lane width used by controllers
H4	Biased/poor lateral state estimation

Step 1 — System-level safety constraints (SC)

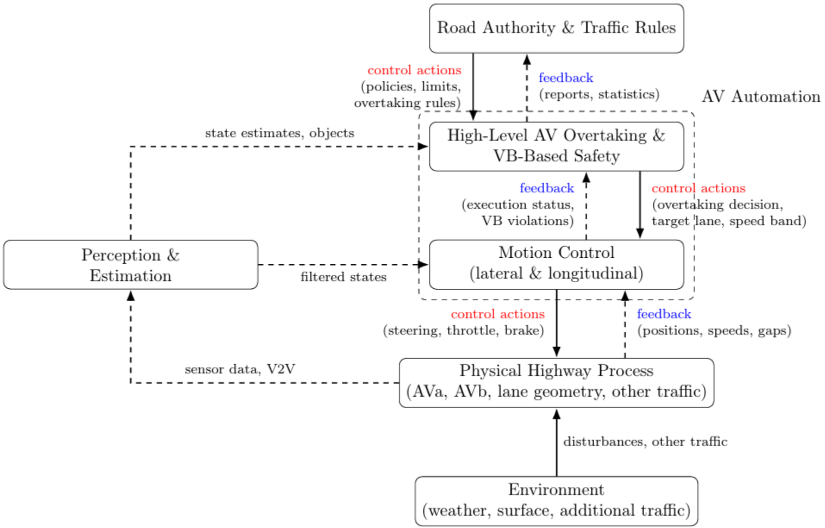
High-level constraints

ID	Constraint
SC1	Maintain sufficient lateral separation for all lane widths
SC2	Maintain sufficient longitudinal separation during overtaking
SC3	Use lane-width estimates consistent with the actual road
SC4	Inhibit/abort overtaking if lateral position uncertainty is too large

Key point

Reduced w makes the system more sensitive to **wrong estimates, delayed updates, and timing errors** in the overtaking decision and control loops.

Step 2 — Control structure (STPA model)



Step 3 — Unsafe Control Actions (UCAs)

UCA definition

An **Unsafe Control Action** is a control action that, in a particular context, can lead to a hazard. STPA classifies UCAs by **how** the action is unsafe:

- Not providing a needed action
- Providing an unsafe action
- Wrong timing/order (too early/late)
- Applied too long / stopped too soon

Why reduced lane widths matter

Narrower lanes reduce tolerance to (i) wrong lane-width estimates, (ii) delayed decisions, and (iii) lateral control overshoot/oscillation.

Key UCAs (examples mapped to hazards)

Representative UCAs from the full table

- **UCA1-1 (authorize overtaking)**: authorize although predicted clearance violates VB limits (H1/H2/H3).
- **UCA2-1 (plan trajectory)**: plan for a wider lane than reality $\Rightarrow$ path violates lateral separation (H1/H3).
- **UCA3-1 (AVa cooperation)**: AVa does not slow down during VB intrusion (H2).
- **UCA4-1 (update lane width)**: outdated w used by VBs/controllers (H3$\rightarrow$H1/H2).
- **UCA5-1 (lane keeping)**: biased lane center $\Rightarrow$ lateral offset toward the other vehicle (H1/H4).

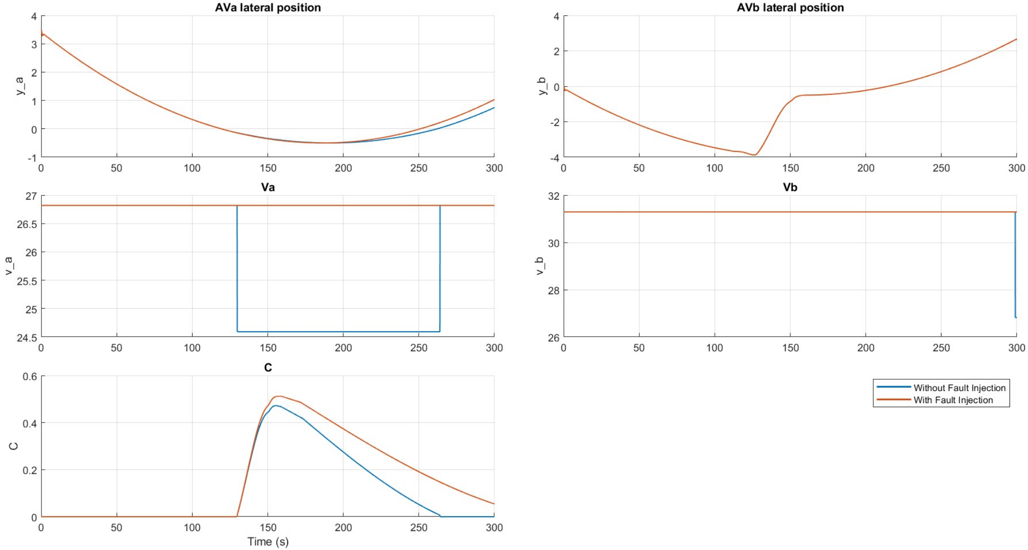
Controller-level safety constraints (derived from UCAs)

ID	Constraint
CC1	Authorize overtaking only if predicted lateral and longitudinal clearances satisfy VB limits for the **current** lane width.
CC2	Issue decisions early enough so the lane-change trajectory respects limits on lateral acceleration and jerk, even in narrow segments.
CC3	AVa shall reduce speed whenever VB intrusion by AVb is detected and maintain minimum headway (longitudinal safety).
CC4	Update VB parameters when lane width decreases; use conservative bounds when perception is uncertain.
CC5	Lateral control shall account for lane-center uncertainty and limit offset/effort to avoid VB violations (steady state + transients).

Engineering view

These constraints are directly translatable into: run-time monitors, controller requirements, and simulation test cases.

Fault injection in simulation — UCA3-1



Overall conclusions

Part I (reproduction)

- Under $S_{nl} = w/2$ and lane-center tracking, w cancels out of the lateral term.
- Reproduction: $C(t)$ almost invariant across w (straight & curved).
- Discrepancy with paper trend suggests missing modeling details.

Part II (STPA + test)

- STPA: hazards arise from unsafe control/feedback, not only failures.
- UCAs $\rightarrow$ explicit controller constraints (CC1–CC5).
- Injecting UCA3-1 shows measurable safety degradation in $C(t)$.

Reproducibility:

`https://github.com/TaharHERRI/Edu-Safety-Analysis-Autonomous-Overtaking`

Q&A

Questions?