

# THE GOVERNANCE GAP

Why Autonomous Systems Need External Authority  
And What Happens If We Don't Build It

**Denzell M. Brown**

Founder and CEO, D3 Dynasty Holdings Inc.

January 2026

## THE INCIDENTS THAT PROVE THE GAP IS REAL

In August 2025, a federal jury in Miami awarded \$243 million to the family of a woman killed when a Tesla operating in Autopilot mode failed to stop at an intersection in the Florida Keys.<sup>1</sup> The jury found Tesla partly liable, not for the crash itself, but for the absence of adequate safety systems and proper warnings. It was the first trial verdict, rather than settlement, against Tesla for an Autopilot-related fatality.

The verdict didn't hinge on whether the driver was paying attention. It hinged on whether Tesla had built sufficient safeguards and accountability into a system that millions of people rely on every day.

Three months later, in December 2025, a Waymo robotaxi in Los Angeles drove directly into an active police felony stop.<sup>2</sup> Officers had a suspect face down on the pavement at gunpoint following a vehicle chase. The driverless Jaguar made a left turn, passed within feet of the prone suspect, and when officers shouted at it to move, briefly turned on its right blinker as if preparing to pull over before eventually clearing the scene.

The officers had no mechanism to assert authoritative conditions the vehicle was required to honor, such as access denial, restricted perimeter enforcement, or entry into a defined minimal-risk state. There was no authenticated way to publish jurisdictional constraints or priority safety conditions that the system could verify and reconcile within its decision space. As a result, the autonomous system continued operating under its default policies, despite the presence of an active law enforcement operation and elevated public safety risk.

**These are not edge cases. These are previews of a systemic failure we have not yet built the infrastructure to prevent.**

## A MOMENT OF CLARITY ON A DARK HIGHWAY

I was seven minutes into scrolling my phone before I realized I was doing it. Twelve-hour shift behind me. Three-hour drive ahead. Somewhere on a stretch of highway I'd driven a hundred times, my body had taken over. Hands on the wheel, foot steady on the gas, eyes technically forward but brain somewhere else entirely. Autopilot. The human kind.

Then I saw the patrol car in my rearview mirror. He'd been behind me for a while. I don't know how long.

I wasn't pulled over. Nothing happened. But a question lodged in my mind that I couldn't shake:

***What happens when a vehicle driving itself has no mechanism to recognize or honor external authority? What if the system has no way to receive authenticated constraints from law enforcement? What if someone is having a medical emergency and no external actor can assert the conditions necessary to bring the vehicle to a safe stop?***

**What happens when the machine has no governance layer to honor?**

That question consumed me. I spent the next several months doing nothing but thinking about it, researching it, and ultimately designing a solution. Not because I saw a business opportunity. Because I realized that if I could solve this problem, I might help keep people alive.

What I found was worse than I expected. The gap isn't just technical. It's architectural. And almost no one is working on it.

## **WHY I SAW IT WHEN OTHERS DIDN'T**

I'm not a software engineer. I'm not from Silicon Valley. I'm a journeyman electrician who spent years climbing cell towers and wiring data centers. That background matters.

When you've climbed a cell tower, you understand that the communications infrastructure everyone takes for granted is physical. It can fail. It can be jammed. It can go dark. When you've wired a data center, you've seen the billions of dollars being poured into AI infrastructure, and you know it's not a bubble. Those buildings are real. That equipment is permanent. This technology is here to stay.

When you've done cutovers at night for T-Mobile, running backup generators so the site stays live while you switch power systems, you understand redundancy. You understand what happens when the primary system fails and there's no backup. You understand that critical infrastructure needs governance that works even when everything else doesn't.

My brain is wired to see systems and patterns. QR codes replacing barcodes. Authentication chains. Constraint hierarchies. How a cabinet talks to a power panel. How a generator keeps a site alive during a transition.

When I asked "what happens when external authority has no way to publish constraints an autonomous vehicle must honor," I wasn't thinking like a software engineer optimizing an algorithm. I was thinking like someone who's spent his career building and maintaining the systems that keep critical infrastructure running.

And what I saw was a gap that no one was filling.

## **THE SCENARIO WE'RE NOT PREPARED FOR**

It's 2028. A major metropolitan area has tens of thousands of autonomous vehicles operating on its streets: a mix of robotaxis, delivery vehicles, autonomous buses, and private AVs from a dozen different manufacturers.

A chemical plant explosion triggers an emergency evacuation of the downtown core.

The city's emergency management office needs to publish constraints that autonomous vehicles must honor: corridor restrictions for emergency vehicle access, geofenced exclusion zones around the contamination area, priority conditions that override normal routing. They need to do this now. Not in twenty minutes. Now.

### **Here's what they discover:**

There is no common interface to publish authenticated constraints to autonomous vehicles from different manufacturers. Each OEM has its own proprietary system with its own protocols. The city has no mechanism to assert jurisdictional authority that vehicles are required to honor. Some vehicles are in autonomous mode with no human occupant to receive a phone call. The cellular network is overloaded, and many vehicles can't reach their cloud infrastructure. There is no way to verify if a constraint was received, authenticated, or reconciled within the vehicle's decision space. There is no record of what conditions were published or how vehicles responded.

### **The city has no governance infrastructure for its own streets.**

This is not science fiction. The Waymo incident in Los Angeles showed us exactly this: officers with no mechanism to publish authoritative conditions that a vehicle was required to honor, no authenticated constraint pathway, and no accountability for the system's continued operation under default policies.

**We are deploying autonomous systems faster than we are building the infrastructure to govern them.**

## **THE ASSUMPTION THAT'S BREAKING DOWN**

The autonomous vehicle industry operates on an unstated assumption: the operator of an autonomous system is the authority over it.

Tesla controls Tesla vehicles. Waymo controls Waymo vehicles. Each manufacturer builds its own governance stack, its own safety systems, its own constraint mechanisms. The assumption is that this is sufficient, that the company that built the system has the right and responsibility to govern it.

This assumption works in a lab. It works on a test track. It even works when autonomous vehicles are rare, experimental, curiosities on public roads.

### **It breaks down completely when autonomous systems become infrastructure.**

When thousands of autonomous vehicles operate in a city, they are no longer just products. They are participants in a shared public space. They interact with traffic systems, emergency services, pedestrians, cyclists, and human drivers. They affect public safety in ways that extend far beyond the relationship between manufacturer and customer.

The police officer who needs to establish a perimeter doesn't care who manufactured the vehicle. The fire department that needs a corridor cleared doesn't have time to call twelve different OEM hotlines. The emergency manager who needs to evacuate a neighborhood can't negotiate with each vehicle's cloud infrastructure.

### **Public authority requires public infrastructure.**

We don't let building owners design their own fire codes. We don't let airlines define their own air traffic control protocols. We don't let banks create their own currency.

Yet we're building a transportation system where every manufacturer defines their own rules for when and how their vehicles honor constraints from public authority.

### **This is the governance gap.**

## THE \$243 MILLION QUESTION

The Tesla verdict wasn't just about one crash. It was about accountability.

The National Highway Traffic Safety Administration found that Tesla's Autopilot system was associated with at least 736 accidents between 2019 and 2023.<sup>3</sup> A federal investigation identified a "critical safety gap" that contributed to at least 467 collisions, including 13 fatal crashes.<sup>4</sup>

But here's what matters for governance: in many of these incidents, there was no clear record of what the system was doing, what constraints it was operating under, what decisions it made, and why. The evidence that existed was controlled by Tesla. The chain of custody for that evidence was opaque.

When the jury awarded \$243 million, they weren't just punishing Tesla for a bad algorithm. They were signaling that manufacturers cannot market autonomous capabilities without building the infrastructure for accountability.

The governance gap isn't just a safety problem. It's a liability problem. It's a regulatory problem. It's a trust problem.

**And it's only going to get worse.**

## WHAT GOVERNANCE ACTUALLY REQUIRES

When I started working on this problem, I assumed someone had already solved it. Surely the engineers at major AV companies had thought about police stops, emergency scenarios, disaster response.

What I found was a patchwork of partial solutions, none of which address the fundamental requirement:

### **Governance is not the same as control.**

Most autonomous vehicles have some form of "minimal risk condition," a programmed response to pull over and stop when certain failures occur. Some have remote operation centers that can take over in edge cases. A few have basic V2X communication capabilities.

None of this constitutes governance. Real governance of autonomous systems requires five things.



## **1. Authenticated Authority**

Any constraint published to an autonomous system must be cryptographically verified. The system must know, with certainty, that the constraint comes from a legitimate authority: not a spoofed signal, not a hacker, not a malicious actor impersonating a police officer.

## **2. Hierarchical Priority**

Not all authorities are equal. A military constraint during a national emergency outweighs a municipal traffic directive. A federal law enforcement restriction takes precedence over a private fleet operator's routing preference. Governance requires a defined, machine-readable hierarchy.

## **3. Execution Verification**

It's not enough to publish a constraint. The publishing authority needs to know: Was the constraint received? Was it authenticated? Was it reconciled within the vehicle's decision space? What was the outcome? This requires bidirectional communication and cryptographic attestation of compliance.

## **4. Tamper-Evident Logging**

Every constraint, every decision, every action must be logged in a way that cannot be altered after the fact. Without reliable logs, liability becomes impossible to determine. Insurance becomes impossible to underwrite. Justice becomes guesswork.

## **5. Denied-Environment Operation**

Governance must work when infrastructure fails. What happens when cellular networks are down? When GPS is jammed? When cloud infrastructure is unreachable? If governance depends on connectivity to a central server, it's not governance. It's a suggestion that works in good weather.

## THE ARCHITECTURE THAT DOESN'T EXIST

As of today, there is no standard architecture that meets these requirements.

There is no common protocol for external authorities to publish authenticated constraints to autonomous vehicles across manufacturers. There is no universal schema for priority conditions and jurisdictional restrictions. There is no cross-vendor interface for emergency services. There is no resilient constraint pathway that operates in denied environments. There is no tamper-evident logging standard for autonomous actions and the authorities that enabled them.

The pieces exist in fragments: V2X communication standards exist, but they focus on safety messages between vehicles, not on authority and governance. Public key infrastructure exists, but it's not integrated into AV constraint pathways. Blockchain technology exists, but it's not applied to autonomous system logging. Military governance doctrine exists, but it's not translated into civilian autonomous systems.

**No one has assembled these pieces into a coherent governance architecture.**

## A FRAMEWORK FOR EXTERNAL AUTHORITY

Over the past year, I've developed and begun patenting an architecture designed to close this gap: a governance layer that sits above autonomous systems and provides the infrastructure for external authority.

I'm not presenting this as a product pitch. I'm presenting it as proof of concept, evidence that the problem is solvable, and a framework for how it might be solved.

**The core insight is simple: autonomous systems need an external governance layer that is independent of any single manufacturer's control stack.**

This layer must accept constraints from authenticated authorities through standardized interfaces, verify those constraints cryptographically including in offline environments, prioritize constraints according to a defined authority hierarchy, reconcile constraints within the vehicle's decision space before high-impact actions, log every constraint and action in tamper-evident form, and operate resiliently when connectivity fails.

This is not about taking control away from manufacturers. It's about ensuring that public authority has a mechanism to publish conditions that autonomous systems are required to honor when public safety requires it.

## **WHO NEEDS TO ACT**

Closing the governance gap requires coordinated action across multiple stakeholders. No single actor can solve this alone.

### **Regulators and Standards Bodies**

We need regulatory frameworks that require, not suggest, external governance capability for autonomous systems operating in public spaces. The regulatory conversation needs to shift from "should autonomous vehicles be allowed" to "what governance infrastructure must they support."

### **OEMs and Fleet Operators**

Manufacturers need to recognize that proprietary governance systems are a vulnerability, not an asset. The \$243 million Tesla verdict should be a wake-up call. The Waymo incident should be a warning. The industry should proactively develop common governance standards rather than waiting for regulation to force fragmented compliance.

### **Emergency Services and Public Safety**

First responders need to be at the table when governance architectures are designed. The LAPD has established a 24/7 hotline for coordinating with Waymo.<sup>5</sup> That's a start, but a phone line is not governance. Law enforcement should be demanding authenticated constraint capability, not just communication channels.

### **Insurers**

The insurance industry has enormous leverage and has barely used it. Insurers can require governance capability as a condition of coverage. They can offer premium reductions for compliant systems. Insurance requirements move markets faster than regulations.

### **Defense and National Security**

Military applications face the governance challenge in its most extreme form: contested environments, adversarial interference, denied communications. Defense investment can accelerate solutions that benefit civilian applications. The military has driven adoption of GPS, the internet, and autonomous flight. It can do the same for autonomous governance.

## THE COST OF WAITING

We have a window to get this right. It won't stay open forever.

Right now, autonomous vehicles are still rare enough that governance failures are manageable. A single Waymo that drives through a police scene is an embarrassment, not a catastrophe. A Tesla verdict is a financial hit, not an existential threat.

That changes as deployment scales. At 10% autonomous vehicle penetration, governance failures become systemic problems. At 30%, they become crises. At 50%, an ungoverned autonomous fleet is a threat to public safety.

And the longer we wait, the harder the problem becomes. Every year of deployment without governance standards means more proprietary systems that resist standardization, more OEMs with incentives to protect their walled gardens, more regulatory fragmentation across jurisdictions, and more incidents that erode public trust.

We've seen this pattern before. Cybersecurity standards came decades after networked systems became ubiquitous, and we're still paying the price. Privacy frameworks came years after data collection became the dominant business model, and they remain inadequate.

We have a chance to do autonomous governance differently. To build the infrastructure before the crisis forces our hand. To design for accountability from the beginning rather than retrofitting it after disasters.

**But that chance requires action now.**

## **CONCLUSION: THE WINDOW IS NOW**

I didn't set out to become a governance architect. I was a tired guy on a long drive who asked a question most people never think about.

But once I saw the gap, I couldn't unsee it. And once I understood that no one was filling it, I felt obligated to try.

The incidents are already happening. A \$243 million verdict for insufficient accountability. A robotaxi operating under default policies through a police standoff with no mechanism for officers to assert authoritative conditions. A regulatory patchwork that can't keep up with deployment.

The architecture I've developed isn't the only possible solution. It's a proof that solutions are possible. A demonstration that the problem is tractable. An invitation to a conversation that the industry, regulators, and public need to have.

Autonomous systems are coming whether we govern them or not. The question is whether we build the infrastructure for accountability before we need it, or after we've learned, painfully, what happens without it.

**The window to choose wisely is now.**

## REFERENCES

1. Hudak, S. "Jury awards \$243 million in Tesla Autopilot death case." NBC News, August 2025.
2. Smith, J. "Waymo robotaxi drives through active LAPD felony stop." ABC News, December 2025.
3. National Highway Traffic Safety Administration. Standing General Order on Crash Reporting: Incident Report Summary. U.S. Department of Transportation, 2024.
4. National Highway Traffic Safety Administration. ODI Resume: Investigation EA 22-002, Tesla Autopilot. Office of Defects Investigation, 2024.
5. Los Angeles Police Department. "LAPD establishes coordination protocols for autonomous vehicle incidents." Press Release, 2025.

## ABOUT THE AUTHOR

**Denzell M. Brown** (known professionally as Zè Monroe) is the Founder and CEO of D3 Dynasty Holdings Inc., a company focused on developing governance architectures for autonomous systems. His work addresses the critical gap between autonomous capability and external authority: authentication, priority resolution, compliance verification, and operation in denied environments.

Prior to founding D3 Dynasty Holdings, **Denzell M. Brown** spent years working in critical infrastructure, where he developed deep expertise in systems that must operate reliably under adverse conditions. This background informs his approach to autonomous governance: systems must work when connectivity fails, when conditions degrade, and when the stakes are highest.

D3 Dynasty Holdings has filed patents covering architectures for autonomous governance, fleet coordination, denied-environment navigation, and compliance logging. The company is open to licensing conversations, standards participation, and strategic partnerships.

## CONTACT

**D3 Dynasty Holdings Inc.**

**Website:** [www.d3dynastyholdings.com](http://www.d3dynastyholdings.com)

**Email:** [ceo@d3dynastyholdings.com](mailto:ceo@d3dynastyholdings.com)

**LinkedIn:** [linkedin.com/in/ze-monroe](https://www.linkedin.com/in/ze-monroe)

---

© 2026 D3 Dynasty Holdings Inc. All rights reserved.

*This document is provided for informational purposes only. The concepts, frameworks, and architectures described herein are protected by pending patent applications filed by D3 Dynasty Holdings Inc. No part of this document constitutes an offer to sell or license intellectual property, nor does distribution of this document grant any rights to the intellectual property described within.*

*This document may be shared for informational purposes with attribution to D3 Dynasty Holdings Inc.*