

AUTOMOTIVE

How heritage automotive brands can compete at software speed



Traditional automakers face a unique challenge that software-first automotive brands don't: reconciling decades of hard-won reputation with the software industry's 'ship and improve' approach. The question now for original equipment manufacturers (OEMs) is how they close the gap to newer, more agile rivals. The race to catch up is far from straightforward, as they must do so without sacrificing the brand image and trust they've spent decades building.

The answer isn't another layer of technology on top of what already exists. It starts with a different question: if we were designing this from scratch, what would we build? That blank-slate mindset is what separates manufacturers that successfully industrialise artificial intelligence (AI), edge and cloud from those that keep adding complexity without gaining speed.



How software-first manufacturers pulled ahead

New market entrants, such as NIO, BYD and Xiaomi, built software-defined platforms designed for continuous evolution from day one. Frequent over-the-air (OTA) upgrades, rapid battery and software iterations and vertically integrated teams have given them a 2-3-year head start with real-world use cases to learn from. Their AI systems, driver-assistance functions and digital cockpits improve with every update.

In the same period, many traditional OEMs have made real progress building connectivity platforms, launching EV architectures and adopting agile methodologies. Though for many, rigid contracts, inherited supplier relationships, and the need to protect profitability in their combustion business has limited their ability to innovate. Despite great technological foundations, the execution gap is widening.

Traditional manufacturers rely on the same off-the-shelf software packages as their competitors, with limited room to differentiate. There's an opportunity to build digital features in house that outperform those third-party solutions. However, this requires a new approach, one that won't succeed unless traditional automakers can overcome the challenges unique to a rich, decades-long heritage.

The challenges

The problem isn't that these OEMs lack technology. It's that each new capability has been added to what came before. This additive approach has created complexity that slows everything down. To differentiate themselves and close the gap to new entrants, they must address four key challenges:

- **Edge computing architecture maturity:** Moving from basic cloud connectivity to sophisticated edge-cloud distribution, while ensuring that public, private and edge systems work together.
- **Organisational integration:** Removing friction between departments to improve software velocity and automotive validation processes.
- **Balancing decision velocity with risk tolerance:** Building technical infrastructure (low-latency, secure, observable) that supports a 'ship and improve' culture while maintaining the quality gates traditional brands require.
- **Using global foundations to deliver better experiences:** Untangling fragmented systems and redesigning them into a unified, compliant edge-cloud platform to reliably support premium, personalised services worldwide.

Moving to a software-first approach would allow traditional OEMs to serve their customers in new ways. However, for this to happen, there needs to be deeper integration across the functional areas of the organisation.



The challenges

Edge computing and risk mitigation

In the plant and across the supply chain, edge enables real-time quality checks, digital twins and mixed-model production without constant retooling. The key is proximity. Processing the information where it's generated reduces latency and ensures simulations run on live data in real time.

Rather than a handful of flagship 'lighthouse' factories, a unified edge-cloud approach allows best-practice applications to be deployed consistently across sites. This catches defects before a vehicle leaves the line and dramatically reduces the cost of poor quality downstream. When you consider that the cost of poor quality rises by three or four times once the vehicle leaves the plant, implementing this technology becomes a cost-saving exercise.

At the vehicle level, the car itself functions as an edge device. High-performance on-board computing manages advanced driver assist systems, battery health, cockpit experiences and AI inference, while regional edge nodes and cloud backends handle heavier analytics, model retraining and OTA orchestration. A common operating layer across private cloud, public cloud and edge turns this into a single platform rather than a collection of disconnected systems. This allows developers to deploy, test and roll back features quickly, with consistent tooling and governance throughout.

The same principle extends to AI deployment. As OEMs move beyond internal use cases into business-critical applications, governance becomes even more important. Which workloads can run on public models, which need localised or air-gapped deployment and how do you enforce consistent policy across all of it? A unified control plane makes scaling AI from pilot to production both safe and fast, giving OEMs the confidence to move quickly without losing visibility or control.

As vehicles and factories become more connected, that architecture is also the natural place to embed security and resilience by design. Modern automotive products sit inside sprawling, partly opaque digital supply chains. The 2024 CrowdStrike outage demonstrated how a single upstream failure can cascade across organisations that had no direct relationship with the affected vendor.

The more durable approach is blank-slate security thinking. Rather than hardening an inherited perimeter, ask how your factories, vehicles and intellectual property should be protected if you were designing from scratch. Zero-trust architecture is built on strong identity, segmentation, least-privilege access and central policy enforcement. Done right, this limits the blast radius, automates recovery and removes the single points of failure that make traditional perimeter-based security so fragile. This security-by-design approach makes faster iteration safe enough to be commercially viable.

Organisational agility: from silos to product thinking

Even with the right platforms in place, many traditional OEMs are constrained by their organisational structure. These weaknesses aren't unique to automotive and are seen across a wide range of industries, including fast-moving consumer goods (FMCG), life sciences and aerospace.

Many of these organisations operate in horizontal silos, each optimising for their own KPIs, tools and timelines. Every hand off between departments requires context to be rebuilt and decisions to be revisited. Even where software teams have adopted agile and modern tooling, the overall product still moves at the pace of the slowest function in the chain.

Software-first automakers organise around products and outcomes rather than departments. Cross-functional teams bring together customer understanding, design, engineering, software and operations under shared accountability for value, quality and speed. For a vehicle programme, the people responsible for digital experience, drive characteristics, manufacturing constraints and lifecycle revenue all work to the same objectives, without the hand-off delays that fragment traditional development.

Moving towards a product-operating model ultimately unlocks the full value of edge, cloud, and AI investment. It reduces the friction that slows iteration, accelerates the journey from pilots to scaled deployment and realigns leadership incentives around software velocity and customer value.

Improved speed without harming quality

To close the gap to software-first manufacturers, traditional brands must move faster. However, this should feel like an extension of their engineering heritage, rather than a desperate push to keep up. With cloud, edge and software-defined vehicle platforms, much more of the development and validation cycle can now happen virtually and continuously. This eliminates slow, one-off physical redesigns.

Digital twins and high-fidelity simulations allow engineers to test new features, calibrations and configurations in days instead of months, long before hardware is committed. When paired with automated testing pipelines and continuous integration/continuous deployment (CI/CD) practices, every change passes through a consistent set of safety, performance and compliance checks before it ever reaches a vehicle.

Once features are in the field, real-time anomaly detection and telemetry at the edge provide an early-warning system that traditional programmes previously didn't have.

The vehicle and surrounding infrastructure can spot unusual patterns in behaviour, failures or usage. It can then either correct them autonomously or flag them for targeted updates. This reduces recalls, lowers the cost of poor quality and catches issues before customers experience them at scale.

This also enables a different narrative: instead of updates being seen as patching a flawed product, OEMs can talk about continuous refinement. The focus can be on regular updates that subtly improve drive feel, personalisation, efficiency and digital services over the vehicle's life. This aligns with the values of many luxury brands.

For this to work, the right foundations must be in place: low-latency infrastructure for safe staged rollouts, zero-trust connectivity ensuring OTA doesn't increase exposure and deep observability showing exactly what changed and where to roll back. With these guardrails, heritage OEMs can increase release cadence without diluting their quality promise.

Using global foundations to deliver better experiences and resilience

As heritage OEMs modernise their architecture and operating models, their global footprint can shift from being a constraint to a source of strength. A well-designed cloud-edge foundation allows manufacturers to place workloads close to customers. This improves performance, keeps data where regulators require it and segments regions so that an incident in one environment does not cascade across the world.

In most cases, this isn't a straight replacement of systems. Legacy infrastructure must be retired progressively as new capabilities mature, protecting continuity and reducing risk.

This has two important knock-on effects. First, it supports more ambitious, software-driven features, such as real-time navigation, intelligent assistants, vehicle-to-everything connectivity, safety services and personalised in-car experiences. These are delivered with the level of reliability and privacy customers expect from a premium brand.

Second, it strengthens business resilience. When identity platforms, monitoring and security policies are designed around zero-trust principles and enforced consistently across regions, the blast radius of an outage or attack is limited and recovery can be automated.

Service outages, production shutdowns and cyber incidents are more visible than ever. The brands that stay up, recover fast and continue to serve customers will deepen trust, turning their global presence and digital maturity into a clear differentiator.



Heritage as an advantage

Software-first competitors have set the pace on iteration, but heritage OEMs own something harder to replicate: global trust, deep engineering capability and brand loyalty shaped over decades. With resilient digital foundations, those strengths don't have to be traded away for the sake of speed.

The brands that will pull ahead aren't those that bolt the most technology onto existing systems, they're the ones willing to ask what they'd build if they were starting today. That blank-slate approach, applied to architecture, security and operating models allows a hybrid edge-cloud foundation to be genuinely transformative rather than another incremental upgrade. It means zero-trust security designed in from the start, product teams with end-to-end accountability and workloads that can move closer to the plant, the vehicle or the cloud as needs evolve.

This unlocks something many software-first manufacturers have struggled to replicate: the combination of iteration velocity and premium experience. Whether that's cars that know their drivers or personalised services delivered with the reliability and privacy a luxury badge demands, it gives a distinct competitive advantage. That is the opportunity facing traditional OEMs willing to move beyond incremental transformation and embrace blank-slate thinking.

This doesn't require scrapping everything and starting afresh. In practice, it's an approach that applies to new investments. Understanding how things might look with a full redesign is important, and new investments should align with this vision, rather than add to ageing architecture.

NTT DATA brings global edge, cloud and AI capability to automotive, logistics, retail and adjacent industries. Whether the solution is on premises, cloud, hybrid, agentic or – as is often the case – all of the above, the focus is always the business outcome: faster launches, fewer recalls, increased lifecycle revenue and a platform that keeps improving long after the vehicle leaves the line.

About NTT DATA

NTT DATA is a \$30+ billion trusted global innovator of business and technology services. We serve 75% of the Fortune Global 100 and are committed to helping clients innovate, optimise and transform for long-term success. As a Global Top Employer, we have diverse experts in more than 50 countries and a robust partner ecosystem of established and start-up companies. Our services include business & technology consulting, data & artificial intelligence and industry solutions, as well as the development, implementation and management of applications, infrastructure and connectivity. We are also one of the leading providers of digital and AI infrastructure in the world. NTT DATA is part of NTT Group, which invests over \$3.6 billion each year in R&D to help organisations and society move confidently and sustainably into the digital future.



Charlie Doubek
Global VP: Agentic AI, Cloud & Security
NTT DATA
<https://www.linkedin.com/in/charlie-doubek>



Lucy Thornton
Managing Director & Head of Cloud & Security, Europe
NTT DATA
<https://www.linkedin.com/in/lucy-thornton>



Deepak Achuthashankar
Global Automotive Solutions & Strategy Leader
NTT DATA
<https://www.linkedin.com/in/deepak-achuthashankar>

Visit us at: nttdata.com



