U ▪ S T | TA TechnologyAdvice

From connected vehicles to trusted intelligence

Scaling AI, securing software-defined architectures, and engineering continuous compliance

ust.com

Contents

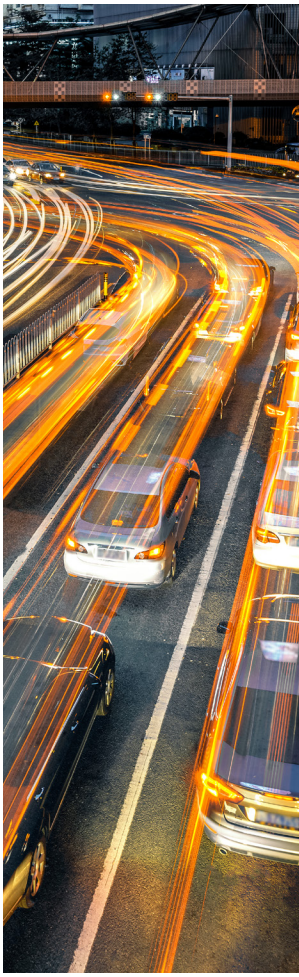
Executive summary: Scaling secure AI across software-defined vehicles

UST surveyed 191 professionals across the automotive ecosystem, including OEMs, suppliers, technology providers, mobility organizations, and cross-industry technology leaders, to assess how the sector is advancing AI, cybersecurity, and software-defined vehicle capabilities. Respondents included CTOs and CIOs, cybersecurity leads, software and platform heads, R&D leaders, product owners, and engineering managers directly responsible for vehicle intelligence and platform strategy.

The findings show strong commitment to AI and connected vehicle transformation—but limited platform-level integration.

The industry is transitioning to software-defined architectures where intelligence influences safety, performance, connectivity, and compliance. For engineering leaders, the question is no longer whether to adopt AI, but how to deploy and govern it securely across complex vehicle systems.

While most organizations view AI and security transformation as drivers of differentiation or disruption, only 10.5% report having fully scaled and integrated AI across the enterprise. More than half remain in early experimentation, and over 40% report partial deployment. In many cases, AI remains concentrated within discrete programs rather than embedded across core architectures.



Cybersecurity risk is escalating alongside AI adoption. Model poisoning ranks as the leading perceived threat, ahead of data privacy breaches and OTA manipulation. Yet only a minority embed security controls from initial design through deployment. In vehicles containing more than 150 electronic control units and layered connectivity stacks, delayed security integration increases validation complexity and systemic exposure.

Software-defined vehicle transformation is advancing, but fleet-level readiness remains constrained. Nearly three-quarters of respondents report that half or fewer of their vehicles support OTA or software-defined capabilities. Skills shortages, regulatory uncertainty, cybersecurity exposure, and legacy ECU architectures continue to limit scale.

Regulatory frameworks such as UNR 155 and ISO/SAE 21434 are further reshaping engineering practices. Few organizations describe themselves as fully compliant and proactive. Compliance now requires continuous traceability across OTA updates, AI model revisions, supplier software components, and cross-border data flows—rendering static certification approaches insufficient.

For CTOs and R&D leaders, the implication is structural. Competitive advantage will depend on integrating predictive safety architectures, embedded cybersecurity, resilient OTA governance, and continuous compliance into a coherent vehicle platform.

This report examines where the industry stands, and what engineering leaders must prioritize to achieve secure, enterprise-scale AI deployment.

Section 1: AI adoption maturity and platform-level integration gaps

AI investment is expanding across automotive product development, manufacturing, and in-vehicle systems. However, survey findings indicate that enterprise-scale integration remains limited.

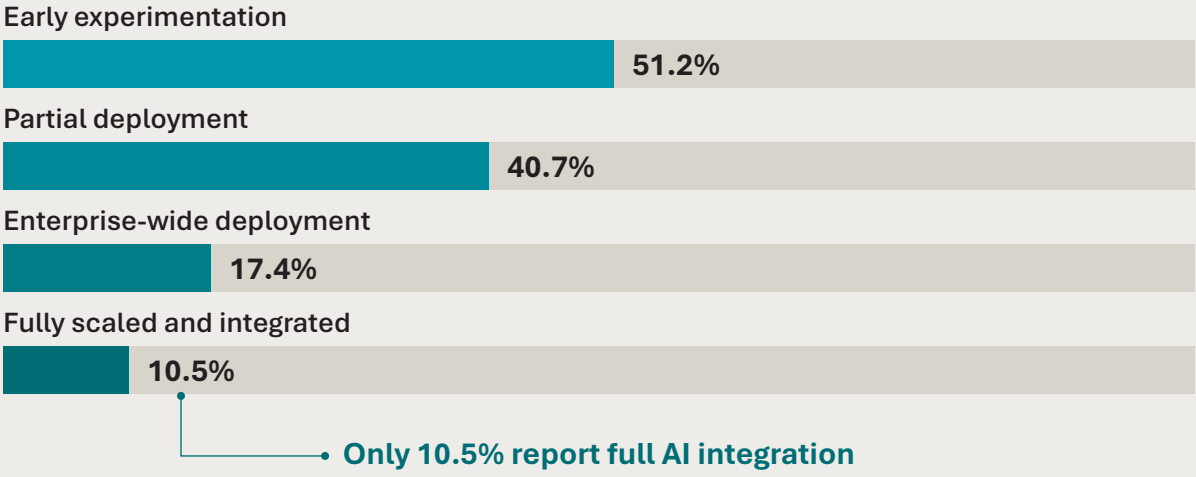
As vehicles evolve into continuously updateable, software-defined platforms, AI must operate as infrastructure: versioned, validated, secured, and integrated across domains. For engineering leaders, the challenge is architectural depth, not experimentation.

AI ambition is widespread.
Platform integration is not

Investment in AI-driven technologies is expanding across product development, manufacturing, and in-vehicle systems. However, survey data reveals a significant maturity gap between experimentation and enterprise-scale integration.

SURVEY QUESTION

"At what stage is your organization in adopting AI-driven technologies across product development, manufacturing, or in-vehicle experiences?"



More than half of organizations remain in the early experimentation stage. Another 40.7% report partial deployment. Only 10.5% indicate fully scaled, integrated AI capabilities across the enterprise.

Even when including enterprise-wide deployments, fewer than one in three organizations have embedded AI at architectural depth. For most respondents, AI remains programmatic rather than platform-level.

The architectural distinction

The survey sample itself reflects a broader industry transformation. More than half of the respondents represent adjacent sectors, including cloud, enterprise security, AI platforms, and connectivity providers. Automotive safety and intelligence are no longer siloed disciplines. They are converging with enterprise-grade software ecosystems.

This cross-industry influence raises expectations. Automotive AI must now meet standards for scalability, governance, and resilience comparable to those of global technology platforms. The transition from experimentation to secure, enterprise-scale intelligence will define which organizations lead the software-defined era.

Section 2: Predictive safety architectures and AI-driven risk mitigation

AI is shifting automotive safety from reactive response to predictive risk modeling. However, investment priorities reveal uneven alignment between safety ambition and architectural depth.

From reactive ADAS to predictive systems

Traditional ADAS systems operate on rule-based logic: detect an object, trigger a response. Predictive systems rely on model-based intelligence. They use sensor fusion — camera, radar, lidar, and contextual data — to anticipate behavior and intervene before risk escalates.

Reactive systems respond. Predictive systems anticipate.

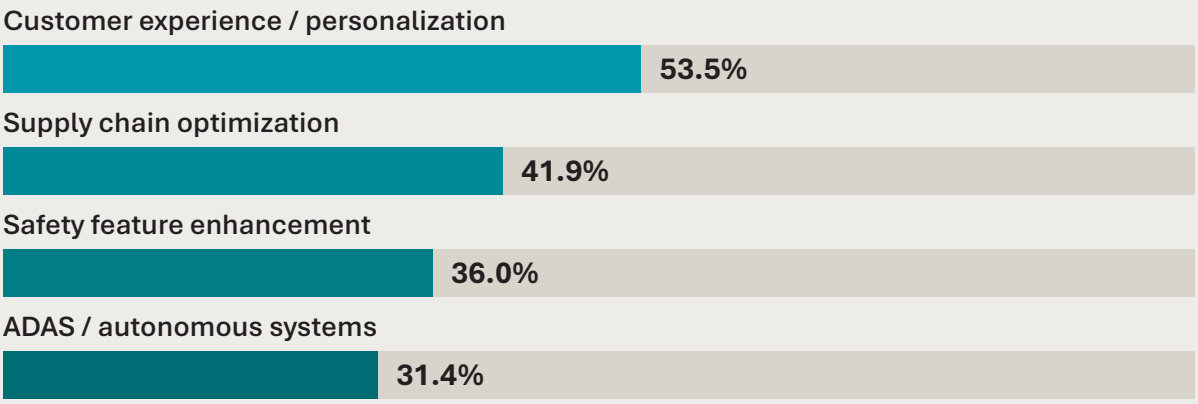
Traditional ADAS (reactive)		AI-powered systems (predictive)
Rule-based “if-then” responses	VS	Model-based environmental intelligence
Responds to immediate obstacles	VS	Builds dynamic 360-degree context using sensor fusion
Millisecond reaction to detected hazard	VS	Predicts intent of pedestrians, vehicles, cyclists
Mitigates collision severity	VS	Prevents dangerous situations from forming

Sensor fusion, combining camera, radar, lidar, and contextual data, enables AI systems to interpret behavior rather than just detect objects. A predictive model can distinguish between a pedestrian standing at the curb and a child moving toward the road. It adjusts before danger escalates. This shift alters the system architecture, not just the feature set.

Investment priorities reveal sequencing

SURVEY QUESTION

“Which areas are receiving the highest AI-related investments?”



Experience leads safety in AI investment priority

Customer experience leads AI investment, followed by operational optimization. Safety-related categories rank lower.

This reflects sequencing rather than neglect. Revenue-generating use cases advance faster than safety-critical architecture, which requires longer validation cycles and deeper system integration. However, predictive safety cannot scale without equivalent investment in model integrity, sensor fusion depth, and secure deployment pipelines.

Section 3: OTA maturity and software-defined vehicle execution constraints

Over-the-air infrastructure is central to software-defined vehicle strategy. However, survey findings indicate that portfolio-level readiness remains limited.

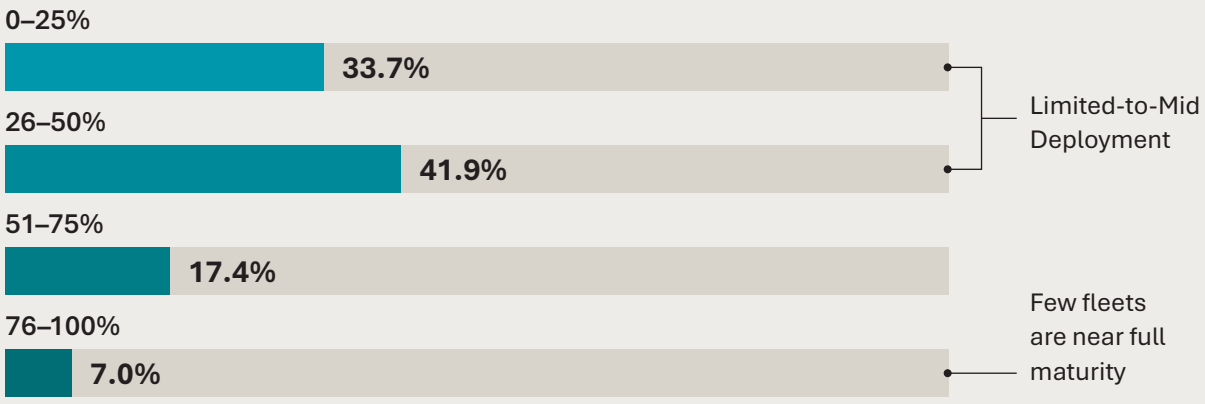
Portfolio support for OTA and SDV capabilities

Software-defined architectures are now central to vehicle platform strategy. Vehicles are becoming increasingly updatable platforms, with performance improvements, safety enhancements, and compliance updates delivered digitally. Over-the-air infrastructure now functions as a strategic supply line for vehicle intelligence.

However, portfolio-level maturity remains limited.

SURVEY QUESTION

"What percentage of your vehicle portfolio currently supports OTA updates or software-defined capabilities?"



Only 7% report high portfolio readiness

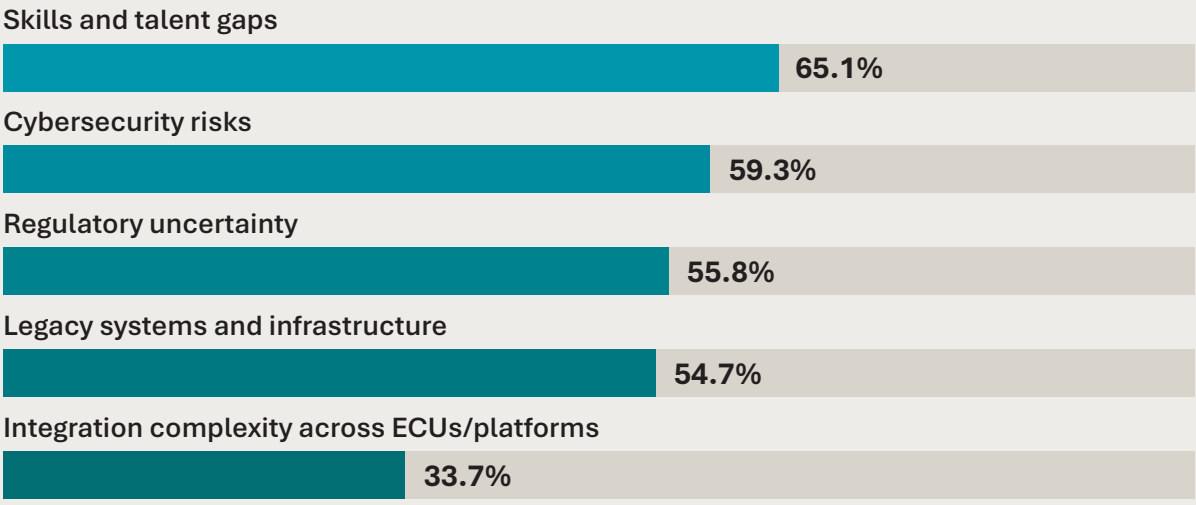
Nearly three-quarters of respondents report that half or less of their portfolio supports OTA or software-defined functionality. Only 7% indicate high fleet-level readiness.

This gap limits the ability to deploy AI updates, security patches, and compliance modifications at scale. Without broad OTA enablement, model iteration and vulnerability remediation remain fragmented across platforms.

Execution barriers to SDV scale

SURVEY QUESTION

"What are the biggest challenges your organization faces in realizing software-defined vehicle (SDV) architectures?"



Execution barriers are organizational and architectural.

Skills shortages rank as the primary constraint. Automotive manufacturers are competing for AI, cloud, and cybersecurity talent in markets already dominated by enterprise technology firms.

Cybersecurity and regulatory uncertainty follow closely, reinforcing that SDV scale is inseparable from secure architecture and compliance readiness. In Nordic markets especially, this is increasingly tied to NIS2 readiness, which is pushing cybersecurity, incident reporting, and executive accountability higher on the automotive software agenda.

Legacy systems present structural friction. Many vehicle platforms were not designed for continuous software iteration. Integrating OTA pipelines into fragmented ECU architectures increases integration complexity, testing overhead, and rollback risk.

OTA is now embedded in safety and compliance

OTA was once considered a convenience feature — primarily for infotainment updates. That framing is obsolete.

Today, OTA pipelines deliver safety patches, AI model updates, cybersecurity mitigations, and regulatory adjustments. A failed deployment can affect thousands or millions of vehicles simultaneously.

This makes rollback capability, cryptographic integrity, update traceability, and variant orchestration non-negotiable requirements. OTA integrity directly affects fleet-level safety, compliance exposure, and operational risk.

Architectural implications

Scaling software-defined vehicles requires coordinated integration across:

- Centralized compute architectures
- Distributed ECU networks
- Secure update pipelines
- Compliance logging systems
- Supplier software validation processes

The survey findings suggest that while the strategic direction toward SDV is established, execution remains constrained by workforce capability, legacy architecture, and cybersecurity complexity.

Organizations that resolve these structural constraints will be positioned to iterate AI models, deploy security mitigations, and adapt to regulatory changes without destabilizing fleet operations.

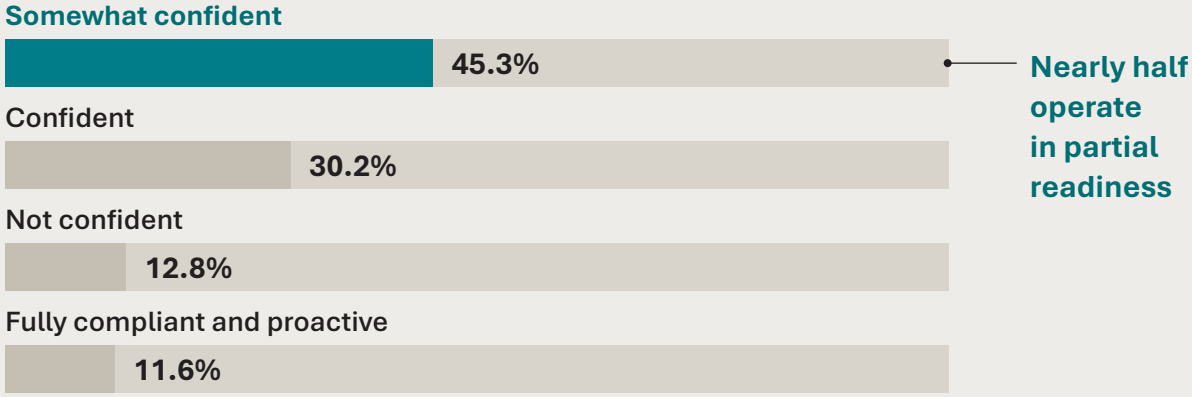
Section 4: Regulatory compliance maturity and continuous traceability gaps

Regulatory requirements are reshaping software architecture and engineering workflows. Survey findings indicate moderate confidence, but limited full-scale readiness.

Confidence under emerging regulatory frameworks

SURVEY QUESTION

"How confident are you in your organization's ability to meet emerging AI and data security regulations in automotive markets?"



Only 11.6% of respondents describe their organizations as fully compliant and proactive. Nearly half report being somewhat confident, indicating partial readiness. More than one in ten lack confidence entirely.

This distribution suggests that, while compliance efforts are underway, most organizations have not yet institutionalized regulatory alignment across architecture, OTA governance, and supplier ecosystems.

Structural barriers to compliance

When asked where compliance efforts face the greatest difficulty, respondents pointed to structural challenges rather than policy interpretation.

SURVEY QUESTION

"Which areas pose the greatest difficulty in achieving compliance with emerging automotive standards?"

Traceability and fragmentation lead compliance friction.

Auditability and traceability are the leading challenges, tied with regulatory fragmentation. This indicates that the primary challenge is not awareness of standards, but the ability to demonstrate compliance in dynamic software environments.

Fragmentation across global regulatory frameworks increases architectural complexity. Engineering teams must accommodate varying regional requirements while maintaining consistent cybersecurity baselines.

Supplier compliance is also a significant constraint. Under frameworks such as UNR 155, OEMs retain accountability for vulnerabilities across third-party software components. This requires deeper visibility into supplier code, update processes, and security validation practices.

From certification milestones to continuous compliance

Vehicles now evolve through OTA updates, AI model revisions, and post-sale feature activation. Static certification models are insufficient for continuously updated platforms.

Continuous compliance requires:

- End-to-end traceability across software versions
- Secure logging of OTA deployments
- Documentation of AI model updates and validation cycles
- Supplier software transparency and vulnerability reporting
- Cross-border data governance controls

Security-by-design becomes an operational requirement rather than a policy objective. Security and compliance controls must be embedded at the architecture level, beginning in early design phases and extending through deployment and lifecycle management.

Engineering implications

For CTOs and R&D leaders, regulatory compliance is increasingly intertwined with system design decisions:

- Centralized versus distributed compute models
- OTA orchestration architecture
- Cryptographic key management strategies
- Supplier integration frameworks
- Data localization and retention controls

The survey findings indicate that most organizations are progressing toward compliance, but full integration of regulatory requirements into software-defined vehicle architectures remains incomplete.

As vehicles become more software-centric and AI-driven, compliance readiness will depend on traceability, update governance, and supplier accountability embedded directly into engineering processes.

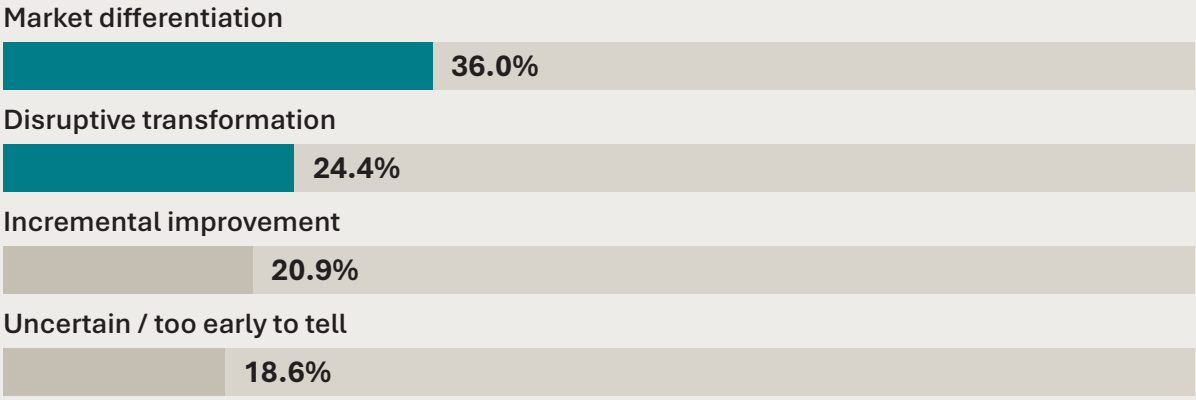
Section 5: Competitive impact of AI and security integration

Survey findings indicate that AI and cybersecurity are viewed not as incremental upgrades, but as structural drivers of competitive positioning.

Strategic impact over the next three years

SURVEY QUESTION

"Which of the following best describes the impact AI and security transformation will have on your competitive positioning over the next three years?"



60.4% view AI and security as strategically transformative.

More than 60% of respondents classify AI and security transformation as either market differentiation or disruptive change. Fewer than one in five view the impact as uncertain.

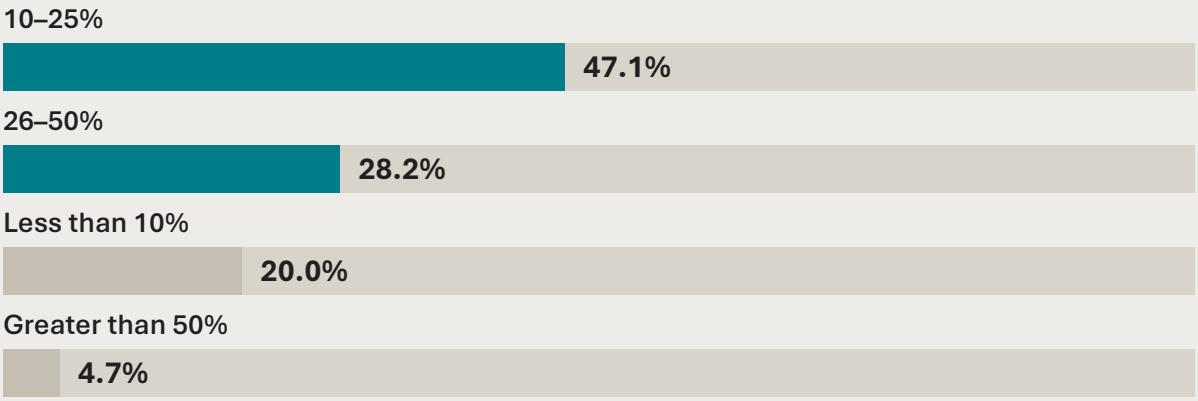
This indicates broad executive alignment that intelligence, cybersecurity, and software-defined capabilities will shape long-term competitiveness.

However, earlier findings in this report highlight maturity gaps in AI integration, OTA scale, and compliance readiness. Strategic intent appears stronger than operational depth.

R&D allocation reflects structural prioritization

SURVEY QUESTION

"What proportion of your R&D budget will be allocated to AI and cybersecurity over the next 24 months?"



Nearly three-quarters allocating double-digit R&D investment.

Nearly three-quarters of respondents plan to allocate between 10% and 50% of R&D budgets to AI and cybersecurity. This level of allocation signals structural reprioritization rather than exploratory spending. Investment levels are substantial, but integration at scale remains the primary constraint.

Strategic themes emerging from the data

Across survey responses, three recurring imperatives emerge:

1. Predictive AI safety architectures over reactive mitigation frameworks
2. Security-by-design embedded from early concept through deployment
3. Continuous compliance integrated into OTA and software lifecycles

These imperatives are interdependent. Predictive AI requires secure data pipelines and update mechanisms. Secure OTA deployment requires cryptographic integrity and rollback controls. Continuous compliance requires traceability across every software release and supplier component.

Fragmented implementation across these domains increases operational friction and validation complexity.

Platform-level integration as competitive constraint

Organizations that treat AI, cybersecurity, OTA, and compliance as separate initiatives will encounter scaling limitations as vehicle architectures become more centralized and compute-intensive.

Competitive advantage will depend on the ability to:

- Integrate AI models across shared compute environments
- Maintain cryptographic integrity across OTA pipelines
- Validate and monitor model performance continuously
- Demonstrate regulatory traceability across global markets

The survey findings suggest that while leadership teams recognize the strategic impact of AI and security integration, achieving architectural coherence across these domains remains uneven.

As software-defined vehicles become the norm, differentiation will be determined less by isolated AI features and more by the resilience, scalability, and governance of the underlying platform.

Conclusion: Engineering secure, scalable AI platforms for software-defined vehicles

Summary

The findings show a consistent pattern: strategic commitment to AI, cybersecurity, and OTA is strong, but platform-level integration remains uneven. Most automotive organizations are advancing these capabilities in parallel, not as a fully coordinated engineering stack. As a result, the central challenge for CTOs and engineering leaders is no longer whether to invest, but how to align architecture, security, update infrastructure, and compliance into a unified operating model.

Key takeaways

- **AI adoption is accelerating, but not always in sync with platform readiness.**
  AI capabilities are expanding across safety systems, digital services, and manufacturing workflows, yet the supporting data, validation, and governance layers often mature at different speeds.
- **Secure OTA depends on more than update capability alone.**
  Effective deployment requires cryptographic integrity, rollback governance, and fleet-level observability to ensure resilience at scale.
- **Compliance is now an architectural issue**
  Regulatory pressure is increasing, and organizations need traceability across software versions, supplier components, and cross-border data flows — not just point-in-time reporting.
- **Fragmented progress creates integration drag.**
  When AI, cybersecurity, OTA, and compliance programs evolve independently, integration complexity increases, validation cycles lengthen, and risk exposure expands.
- **Competitive resilience will come from platform coherence.**
  The next phase of automotive transformation will be defined less by standalone AI features and more by the ability to integrate intelligence, cybersecurity controls, update infrastructure, and compliance processes into one engineering framework.
- **Architectural discipline is becoming the priority.**
  For organizations navigating software-defined vehicle transformation, the focus must shift from incremental enhancement to embedding security, traceability, and scalability directly into vehicle platforms from design through deployment.
- **Sustainable differentiation will depend on secure scale.**
  As vehicles become more software-centric and compute-intensive, long-term advantage will come from the ability to deploy, update, validate, and govern intelligent systems across the full vehicle lifecycle.