CAAR | IIT Madras

Centre of Excellence for Advanced Automotive Research

Global Automotive AI, SDV & Cybersecurity Outlook

FEBRUARY 2026

Software-Defined Vehicles · AI & ADAS · Cybersecurity

Electrification · Lifecycle Trust

Global Automotive AI, SDV & Cybersecurity

Whitepaper February 2026

**Author: Srinivas Mahankali, Armour1X LLP &
Dr. Anand Lakshmanan, CAAR with inputs from
Major. Vineet Kumar, CyberPeace**

Centre of Excellence in Advanced Automotive Research (CAAR)

**3rd Floor, NCCRD Building,
Indian Institute of Technology Madras,
Chennai - 600036, Tamil Nadu, India**

Contents

Foreword

Thiruppathy Srinivasan, Chief Executive Officer, CAAR - https://CAAR.tech

The automotive industry is entering a decisive decade. The convergence of **software-defined vehicles, artificial intelligence, cybersecurity, electrification, and lifecycle regulation** is fundamentally redefining how vehicles are designed, manufactured, deployed, and governed. This transformation is not incremental; it is architectural.

For India, this moment presents both opportunity and responsibility. Our manufacturing scale, engineering talent, and growing digital infrastructure provide a strong foundation. Yet global competitiveness in the coming decade will be determined not merely by volume, but by **system-level** capability—the ability to design resilient architectures, ensure cybersecurity and AI safety, manage software lifecycles, and align continuously with global standards.

CAAR was established to operate at this intersection of technology depth, industry relevance, and institutional trust. This whitepaper reflects our conviction that India requires a neutral, technically credible automotive technology nerve center—one that orchestrates platforms, reference architectures, validation frameworks, certification systems, and talent development across the ecosystem.

This document is not a projection of trends alone. It is a call for coordinated action—by industry leaders, policymakers, academia, and global partners—to build enduring capability rather than fragmented excellence. CAAR is committed to playing this role with rigor, openness, and long-term intent.

Message from IIT Madras Leadership

Prof V. Kamakoti, Chairman, CAAR

Over the past decades, IIT Madras has consistently focused on translating academic excellence into national impact. As technologies mature faster and system complexity increases, the role of leading academic institutions must evolve—from centers of research to **anchors of ecosystem capability**.

Mobility is now a cyber-physical, software-intensive, and energy-integrated system. Addressing its challenges requires **interdisciplinary collaboration**, long-horizon thinking, and trusted institutional platforms that can engage industry and government with equal credibility.

CAAR represents this evolution in action. Situated within the IIT Madras ecosystem, while being an independent Research Society, it brings together engineering depth, applied research, industry engagement, and global standards alignment. Its identity as an independent research society is suited to take the lead in bringing together the top minds in the academic institutions in the country and beyond. This whitepaper demonstrates how such an institution can contribute not only to innovation but to **stability, safety, and global relevance**.

IIT Madras strongly supports CAAR's vision of serving as a national and global reference point for advanced automotive technologies. The institute views this effort as aligned with its broader mission: enabling India to lead responsibly in technologies that shape society, industry, and sustainability.

Vision Statement from the CAAR Governing Council

The next phase of automotive evolution will be defined by **trust**—trust in software, trust in AI decisions, trust in cybersecurity resilience, and trust in lifecycle integrity. This trust cannot be established by individual organizations acting in isolation. It requires i**nstitutional frameworks** that endure beyond product cycles and technology waves.

The Governing Council of CAAR envisions the Centre evolving into **India's Automotive Technology Nerve Centre** — a role defined by orchestration rather than ownership, by enablement rather than control.

Our vision is that CAAR will:

- Rework and **establish new technology and standards** in Stability, vehicle dynamics, suspension, and braking including for off-road vehicles
- Define and steward **reference architectures** for software-defined and AI-native vehicles
- Anchor **cybersecurity, AI safety, and OTA governance** as core automotive disciplines
- Enable **globally aligned certification and validation frameworks**
- Support **talent and leadership development** for system-level automotive roles
- Represent India meaningfully in **global standards and technology dialogues**

This whitepaper articulates a roadmap toward that vision. Its success depends not on CAAR alone, but on the collective commitment of industry, government, and academia to build shared platforms for long-term national advantage.

Why This Whitepaper, Why Now

The period from **2026 to 2035** will define the global automotive hierarchy for generations. Several forces make this moment uniquely consequential:

- **Vehicle dynamics** is undergoing significant shifts as the Automotive industry is going through a major revolution
- **Software-Defined Vehicles** are shifting value from hardware to code, data, and platforms
- **AI and ADAS** are introducing probabilistic decision-making into safety-critical systems
- **Cybersecurity and OTA regulations** are becoming prerequisites for market access
- **Electrification and battery traceability mandates** are reshaping supply chains and compliance
- **Global standards density** is increasing faster than industry's ability to absorb it.

For India, the risk is not lack of capability, but **fragmentation**—isolated excellence without system-level coherence. Without shared architectures, validation platforms, and certification frameworks, innovation becomes slower, costlier, and riskier.

This whitepaper has been developed to:

- Provide a **clear, integrated view** of global automotive technology shifts
- Assess India's current ecosystem readiness with candor
- Articulate the **institutional role required** to bridge gaps at scale
- Define a **10-year roadmap** for capability building and global leadership

The intent is not advocacy, but **alignment**. Not speculation, but **execution clarity**.

Section 1
The Global Automotive Industry Reset (2020–2035)

From Mechanical Engineering to Software-Defined, Cyber- Physical Mobility

1.1 The End of the Traditional Automotive Paradigm

For more than a century, automotive competitiveness was defined by mechanical engineering excellence, manufacturing scale, and supply-chain efficiency. That paradigm is now structurally obsolete.

Between 2020 and 2035, the automotive industry is undergoing a **once-in-a- generation reset**, driven not by incremental innovation but by a fundamental reallocation of value—from hardware to software, intelligence, and lifecycle services.

What distinguishes this transition from prior technological cycles is **irreversibility**. Unlike past waves (electronics, infotainment, basic ADAS), today's shifts are reinforced simultaneously by:

- Regulation
- Economics
- Consumer expectations
- Technology convergence

As a result, the industry is no longer converging on a single dominant product architecture, but on a **software-centric operating model**.

1.2 Five Structural Shifts Redefining the Industry

Shift 1: From Vehicle as a Product to Vehicle as a Software Platform

Global OEMs are rapidly abandoning distributed, ECU-heavy architectures in favor of **centralized and zonal computing platforms**.

This shift enables:

- Continuous over-the-air (OTA) upgrades
- Decoupling of hardware and software lifecycles
- Faster feature deployment and monetization
- Unified cybersecurity and safety governance

Implication:

Competitive advantage is shifting from component optimization to **software architecture ownership**.

Shift 2: From Embedded Software to AI-Native Automotive Systems

AI is no longer confined to perception and ADAS. Leading OEMs and suppliers are embedding AI across the full automotive value chain:

- **R&D:** Generative design, simulation, digital twins
- **Manufacturing:** AI-driven quality, yield optimization, predictive maintenance
- **In-Vehicle:** Perception, driver monitoring, personalization
- **Lifecycle:** Predictive degradation, warranty fraud detection, second-life optimization

AI is increasingly **agentic**, autonomous, and embedded into decision loops previously handled by human engineers.

Implication:

Automotive competitiveness increasingly depends on **AI model maturity, data pipelines, and validation frameworks**, not just algorithm availability.

Shift 3: From Functional Safety to Cyber-Physical Resilience

Historically, safety was governed by mechanical redundancy and deterministic systems. Today's vehicles are **networked cyber-physical systems**, exposed to adversarial threats.

Key characteristics of the new risk landscape:

- Wireless attack surfaces (Bluetooth, UWB, V2X)
- OTA and firmware manipulation risks
- CAN and Ethernet message injection
- AI model poisoning and sensor spoofing Cybersecurity is now inseparable from:
  a. Functional safety
  b. Brand trust
  c. Regulatory compliance

Implication:

Cybersecurity is no longer an IT function—it is a **core engineering discipline and homologation requirement**.

Shift 4: From Electrification to Energy Integration

Electrification is no longer limited to replacing internal combustion engines. Vehicles are becoming **active nodes in distributed energy systems**.

Emerging global models include:

- Vehicle-to-Grid (V2G) integration
- Second-life battery markets
- Grid-stabilization services

- Circular material recovery

Implication:

Energy intelligence and lifecycle traceability are becoming strategic capabilities, not compliance overheads.

Shift 5: From Linear Supply Chains to Lifecycle Trust Platforms

Regulation and market expectations are forcing a transition from opaque supply chains to **digitally verifiable lifecycle systems**.

Global mandates increasingly require:

- Component traceability
- Software update auditability
- Carbon and sustainability reporting
- End-of-life accountability

Implication:

Trust, compliance, and transparency are becoming **digitally encoded capabilities**, not manual processes.

---

13 Exhibit: Global Automotive Value Pool Shift

Exhibit 1: Automotive Value Distribution (Indicative, % of Total Value)

Value Driver	2005	2020	2035 (Projected)
Mechanical Hardware	65%	45%	25%
Embedded Software	15%	20%	15%
AI & Digital Systems	5%	15%	25%
Data & OTA Services	5%	10%	20%
Energy & Lifecycle Services	10%	10%	15%

Key Insight:

By 2035, **over 60% of automotive value is expected to be software-, data-, and energy-driven**, fundamentally altering profit pools and competitive dynamics.

---

14 Benchmark: R&D Intensity as a Leading Indicator

R&D intensity is emerging as one of the most reliable proxies for future competitiveness—particularly when R&D is disproportionately allocated toward software, AI, and cybersecurity.

Exhibit 2: R&D Spend as % of Revenue (2023–24)

Segment	R&D Intensity
Global SDV-First OEMs	8–12%
Traditional Global OEMs	5–7%
Automotive Technology Majors	10–15%
Indian OEMs (Average)	2-4%

Additional Observation:

In leading SDV programs, **over 50% of R&D spend is now software- and AI- oriented**, compared to less than 25% in most emerging-market OEMs.

15 Implications for Emerging Automotive Ecosystems

For countries and ecosystems outside the traditional automotive strongholds, the reset creates both risk and opportunity.

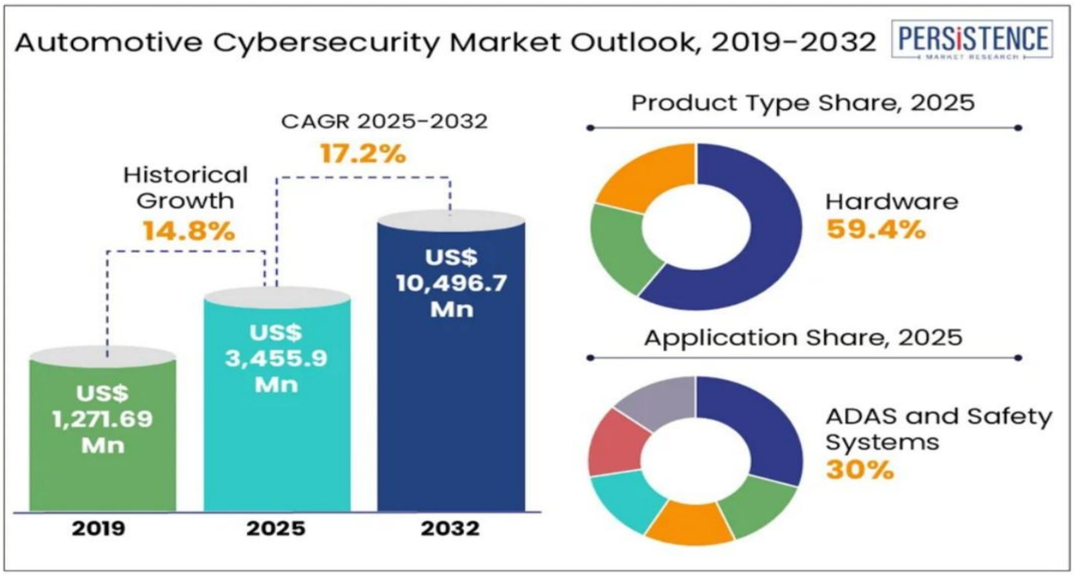
Risks

- Structural dependence on foreign SDV stacks
- Loss of value capture despite manufacturing scale
- Regulatory barriers to exports due to cybersecurity non-compliance

Opportunities

- Leapfrogging legacy architectures
- Building software-first platforms natively
- Institutional leadership in validation, certification, and trust

Crucially, these opportunities cannot be realized through individual firms alone. They require **shared platforms, neutral institutions, and ecosystem orchestration**.



1.6 Why Institutional Capability Matters

Global experience demonstrates that no automotive ecosystem has transitioned successfully to the SDV era without **strong institutional anchors** that provide:

- Reference architectures
- Validation and certification
- Talent pipelines
- Standards alignment
- Neutral collaboration platforms

This reality frames the central question for India:

Who will own the system-level capabilities that individual OEMs and startups cannot economically build alone?

The remainder of this report addresses that question—and the role CAAR can play in answering it.

Section 2
Software-Defined Vehicles (SDV): Global Architecture & Implications

Re-architecting the Vehicle Around Software, Compute, and Continuous Evolution

2.1 SDV Architecture Evolution

From ECU Proliferation to Centralized Compute

For decades, vehicle electronic architectures evolved incrementally, driven by feature addition rather than system design. Each new function—ABS, airbags, infotainment, ADAS—added a dedicated Electronic Control Unit (ECU). This resulted in **ECU sprawl**, with modern vehicles containing 70–120 ECUs,
interconnected through heterogeneous buses.

This architecture is now economically and technically unsustainable.

Global OEMs are transitioning through three distinct architectural phases:

Phase 1: Distributed ECU Architecture (Legacy)

Characteristics

- Function-specific ECUs
- Tight coupling of hardware and software
- Point-to-point integrations
- Limited OTA capability

Limitations

- High wiring complexity and weight
- Slow feature deployment cycles
- Fragmented cybersecurity posture
- Escalating integration costs

Phase 2: Zonal Architecture (Transitional)

Characteristics

- ECUs grouped by physical zones (front, rear, cabin)
- Zonal controllers aggregate sensor and actuator data
- Reduced wiring harness complexity

Benefits

- Cost and weight reduction
- Improved fault isolation
- Early enabler of OTA updates

Constraints

- Still reliant on multiple compute islands
- Partial abstraction of software from hardware

Phase 3: Centralized Compute Architecture (SDV-Native)

Characteristics

- High-performance central compute units
- Vehicle functions implemented as software services
- Decoupled hardware–software lifecycles
- Cloud-connected, OTA-first design

Strategic Advantage

- Faster innovation cycles
- Unified cybersecurity governance
- Platform-level monetization
- Scalable AI deployment

Key Insight:

SDVs are not defined by OTA capability alone—they are defined by **architectural decoupling** and **software control over vehicle behavior**.

Vehicle OS, Middleware & API Economies

The Automotive Software Stack Is Being Rewritten

In SDV architectures, the vehicle increasingly resembles a **distributed computing platform**, with a layered software stack:

1. **Hardware Abstraction Layer (HAL)**
   Abstracts sensors, actuators, and computer hardware
2. **Vehicle Operating System (Vehicle OS)**

   Manages compute resources, real-time constraints, and safety isolation
3. **Middleware & Service Frameworks**

   Enables inter-process communication, data sharing, and OTA orchestration
4. **Application & Feature Layer**

ADAS, infotainment, energy management, personalization

5. **Cloud & DevOps Integration**
   Continuous deployment, diagnostics, analytics, and AI model updates This shift enables **API-driven vehicle functionality**, where features are composed, updated, and monetized like software products.

Implication:

Control over the Vehicle OS and middleware layer is emerging as the **single most critical leverage point** in the SDV ecosystem.

2.2 Monetization Models in the SDV Era

The SDV transition fundamentally alters how value is created and captured over a vehicle's lifetime.

Feature-as-a-Service (FaaS)

Instead of bundling features at the point of sale, OEMs increasingly offer:

- Subscription-based ADAS enhancements
- Performance upgrades
- Comfort and personalization features

Benefits

- Continuous revenue post-sale
- Personalization at scale
- Data-driven pricing strategies

Constraint

- Requires robust software architecture, telemetry, and customer trust

---

OTA-Driven Revenue Streams

OTA updates are evolving from maintenance tools into **commercial enablers**:

- Paid feature unlocks
- Regulatory updates without recalls
- AI model upgrades (e.g., perception improvements)

Strategic Impact

- Reduction in recall costs
- Extension of vehicle economic life
- Faster regulatory compliance

Data & Platform Economics

SDVs generate large volumes of high-value data:

- Vehicle health and usage
- Driver behavior (where permitted)
- Energy consumption patterns
- Fleet optimization signals

Leading OEMs are building **closed-loop data platforms** to:

- Improve product design
- Optimize manufacturing
- Enable ecosystem partnerships (insurance, energy, mobility services)

Key Insight:

Data monetization is less about selling data and more about **embedding data into decision advantage and service differentiation**.

---

23 Implications for Indian OEMs & Tier-1 Suppliers

Strategic Implications for Indian OEMs

Indian OEMs face a dual challenge:

- Competing in a global SDV-dominated market
- Managing cost sensitivity in a price-constrained domestic market

Key Implications

1. **Architecture Decisions Are No Longer Optional**

   SDV-ready platforms must be designed early, not retrofitted.

2. **Software Capability Must Be Core, Not Outsourced**

   Excessive reliance on third-party stacks risks long-term margin erosion.

3. **Cybersecurity and OTA Readiness Are Export Prerequisites**

   Non-compliance increasingly restricts access to global markets.

Implications for Tier-1 & Tier-2 Suppliers

The SDV transition is reshaping supplier economics:

- Hardware-only suppliers face commoditization
- Software-enabled suppliers gain pricing power
- Tier-1s are expected to deliver integrated systems, not components

Emerging Success Factors

- Software-defined subsystems

- Cybersecurity-certified modules
- OTA-compatible architectures
- AI-enabled diagnostics and updates

Exhibit 3: Architecture Comparison – Traditional vs SDV Stack

Traditional Vehicle Stack

- Hardware-bound ECUs

Function-specific software

- Limited OTA
- Fragmented security controls

SDV Stack

- Centralized compute
- Vehicle OS and middleware
- API-driven features
- Unified cybersecurity governance
- Cloud-native lifecycle management

Key Difference:

In SDVs, **software defines the vehicle**; hardware becomes an execution substrate.

Exhibit 4: Benchmark – Software Revenue per Vehicle (Indicative)

OEM Category	Software Revenue per Vehicle (Lifetime)
Global SDV Leaders	USD 1,500 – 3,500
Traditional Global OEMs	USD 500 – 1,000
Emerging Market OEMs	USD 300
Indian OEMs (Current Avg.)	USD 200

Projection:

By 2035, software-led revenue is expected to exceed **25–30% of total vehicle lifetime value** for leading OEMs.

2.4 Institutional Orchestration in the Software-Defined Vehicle Era

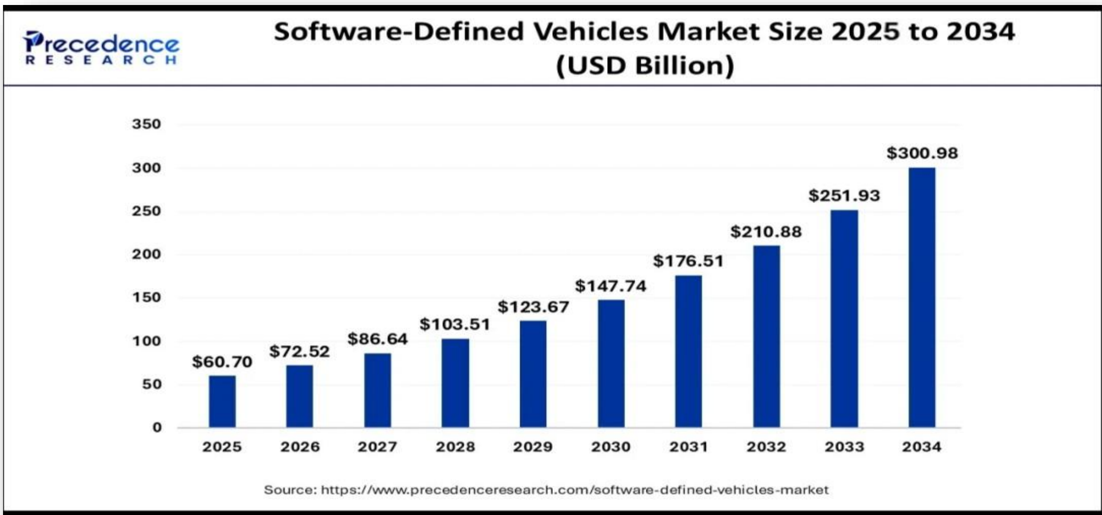
The transition to software-defined vehicles is not merely a technological shift but an ecosystem-level transformation. Modern SDV architectures rely on complex combinations of vehicle operating systems, middleware, embedded software, AI workloads, digital cockpit frameworks, and cloud-connected development workflows. While global technology providers offer increasingly sophisticated SDV building blocks, the integration, validation, and governance of these components across the vehicle lifecycle has emerged as a critical challenge for OEMs and suppliers alike.

As vehicles become programmable platforms, the primary risk shifts from individual component failure to system-level integration risk—spanning cybersecurity, functional safety, software updates, and regulatory compliance. Addressing this risk requires neutral, institutional orchestration that can define reference architectures, enable multi-vendor interoperability, and provide trusted validation environments without creating vendor lock-in. Globally, automotive ecosystems that successfully navigate the SDV transition are those supported by strong institutional anchors that operate above individual technologies and commercial interests.

2.5 Strategic Takeaways

1. **SDV is an architectural transformation, not a feature upgrade**
2. **Software platforms, not vehicles, will define competitive advantage**
3. **Late architectural decisions impose long-term economic penalties**
4. **Institutional support is required to de-risk SDV transitions at scale**

These realities reinforce the need for **shared reference architectures, validation platforms, and talent pipelines**—a theme developed further in subsequent sections of this report.



Section 3
Artificial Intelligence as the New Automotive Engine

From Embedded Intelligence to AI-Native Automotive Systems

3.1 AI Across the Automotive Value Chain

Artificial Intelligence is no longer an incremental enhancement within automotive systems. It is becoming the **primary engine of differentiation**, reshaping how vehicles are designed, built, operated, secured, and monetized.

Leading automotive players are no longer asking *where* to apply AI—but *how to re-architect the enterprise* around AI-driven decision loops.

Design, Simulation & Digital Twins

AI is transforming early-stage vehicle development from a sequential, human- intensive process into a **continuous, simulation-driven workflow:**

Key applications include:

- **Generative design** for structural components and assemblies
- **AI-accelerated simulation** reducing physical prototyping cycles
- **Digital twins** of vehicles, subsystems, and manufacturing lines

Impact

- Reduction in design-to-prototype timelines (30–50%)
- Improved performance-to-weight optimization
- Earlier detection of safety and compliance risks

Strategic Shift:

Design intelligence is moving upstream—embedding manufacturability, safety, and lifecycle considerations from inception.

AI-Driven Manufacturing

Manufacturing is emerging as one of the **highest-ROI domains for applied AI** in automotive.

Core applications include:

- Computer-vision-based quality inspection
- Predictive maintenance for critical equipment
- Yield optimization and scrap reduction
- Autonomous process control and tuning

Unlike traditional automation, AI-driven manufacturing systems **learn continuously** from production data.

Impact

- 20–40% reduction in defect rates
- Higher first-time-right manufacturing
- Lower recall and warranty exposure

Key Insight:

AI shifts manufacturing from reactive quality control to **predictive and preventive quality engineering**.

In-Vehicle AI & Personalization

Within the vehicle, AI capabilities are expanding beyond ADAS into:

- Driver monitoring and behavior modeling
- Context-aware infotainment and comfort systems
- Energy optimization and range intelligence
- Adaptive safety systems

These systems rely on **real-time inference at the edge**, combined with cloud- based learning loops.

Constraint:

Trust, privacy, and cybersecurity increasingly determine customer acceptance and regulatory approval.

Lifecycle Intelligence

Perhaps the most underappreciated impact of AI lies in **post-sale lifecycle management**.

AI enables:

- Predictive degradation modeling
- Early detection of failure patterns
- Warranty fraud identification
- Second-life and end-of-life optimization

Impact

- Lower warranty costs
- Reduced unplanned recalls
- Higher residual value management

Strategic Shift:

The vehicle lifecycle is becoming a **continuously optimized system**, not a static depreciation curve.

3.2 Generative AI & Agentic AI in Automotive

From Assistive Tools to Autonomous Decision Agents

The automotive industry is entering a new phase of AI adoption characterized by **Generative AI and Agentic AI**—systems that do not merely analyze data, but **generate designs, decisions, and actions**.

Design Automation

Generative AI models are now capable of:

- Producing CAD-ready component designs
- Exploring thousands of design permutations
- Optimizing across performance, cost, and manufacturability constraints

Result

- Faster innovation cycles
- Democratization of advanced design capabilities
- Reduced dependence on scarce specialist skills

Autonomous Quality Inspection

AI vision systems increasingly outperform human inspectors in:

- Detecting micro-defects
- Identifying process drift
- Classifying root causes autonomously

When combined with agentic control systems, AI can:

- Adjust process parameters in real time
- Trigger corrective actions without human intervention

Predictive Warranty & Recall Prevention

By correlating vehicle telemetry, production data, and field incidents, AI agents can:

- Identify emerging failure patterns
- Recommend targeted software or hardware interventions
- Prevent mass recalls through localized corrective action

Key Insight:

Generative and agentic AI transform quality and warranty from cost centers into **strategic control levers**.

3.3 Why AI Sovereignty Matters for India

As AI becomes foundational to automotive competitiveness, **dependence on external AI stacks introduces systemic risk**.

Key Dimensions of AI Sovereignty

1. **Architectural Control**

   Dependence on proprietary, black-box AI platforms limits transparency and adaptability.

2. **Data Governance**

   Automotive data is safety-critical, commercially sensitive, and increasingly regulated.

3. **Skill & Capability Retention**

   Outsourcing core AI systems erodes long-term engineering capability.

4. **Regulatory & Export Readiness**

   Explainability, auditability, and certification of AI systems are becoming mandatory.

Strategic Implication:

AI sovereignty is not about isolation—it is about **capability ownership, validation, and trust**.

Exhibit 5: AI Use-Cases by Automotive Function

📊 **Chart: AI Penetration Across the Automotive Value Chain**

Automotive Function	AI Adoption Maturity
Design & Simulation	High
Manufacturing & Quality	High
ADAS & Perception	Medium–High
Energy & Battery Management	Medium
Lifecycle & Warranty	Medium
Supply Chain & Logistics	Emerging

Observation:

AI adoption is deepest where data density and economic impact intersect.

Exhibit 6: Automotive AI Maturity Model

Maturity Model: Automotive AI Adoption Levels

Level 1 - Rule-Based Automation

- Deterministic logic
- Minimal learning capability

Level 2 - Assisted Intelligence

- AI supports human decision-making
- Limited autonomy

Level 3 - Predictive Intelligence

- AI forecasts failures and outcomes
- Human-in-the-loop control

Level 4 - Autonomous Intelligence

- AI systems take corrective actions
- Closed-loop learning systems

Level 5 - Agentic & Self-Optimizing Systems

- AI agents generate designs, decisions, and actions
- Continuous self-improvement across lifecycle

Current Position

- Global Leaders: Level 3–4
- Most Emerging OEMs: Level 1–2

Target State (2035):

AI-native automotive enterprises operating at **Level 4–5 maturity**

3.4 Strategic Takeaways

1. **AI is now a core automotive system—not a feature**
2. **Value accrues to those who control AI architectures, not just algorithms**
3. **Generative and agentic AI redefine speed, quality, and cost curves**
4. **AI sovereignty underpins long-term competitiveness and trust**

These dynamics reinforce the need for **shared AI testbeds, validation frameworks, talent pipelines, and institutional oversight**—capabilities that individual firms cannot efficiently build alone.

Section 4
Autonomous Driving & ADAS: From Capability to Resilience

Why the Next Decade Will Be Defined Less by Autonomy Levels and More by System Robustness

4.1 Global Reality Check on Autonomy

Over the last decade, autonomous driving has been one of the most heavily capitalized and publicly discussed domains in the automotive industry. Yet despite significant investment, the industry's progress toward full autonomy has been **non-linear and uneven**.

While technical capabilities have advanced, **deployment reality has been constrained** by safety, regulatory, cost, and resilience considerations.

What Has Materialized

- Widespread deployment of Level 2 and Level 2+ ADAS
- Limited, geo-fenced Level 3 deployments in controlled conditions
- Experimental Level 4 pilots in constrained environments (e.g., robo-taxi corridors)

What Has Not

- Scalable, consumer-grade Level 4/5 autonomy
- Robust handling of long-tail edge cases
- Universal regulatory approval across markets

Key Insight:

The bottleneck to autonomy is no longer perception accuracy alone—it is **system-level reliability under uncertainty**.

4.2 ADAS Proliferation & the Software Safety Imperative

As full autonomy remains elusive, **ADAS has emerged as the dominant pathway** through which intelligence is entering vehicles at scale.

Why ADAS Is Scaling Faster Than Autonomy

- Clear safety benefits
- Incremental deployment model
- Easier regulatory acceptance
- Strong consumer demand

ADAS features such as adaptive cruise control, lane keeping, automatic emergency braking, and driver monitoring are now standard or near-standard across segments.

However, this proliferation introduces a new challenge:

ADAS systems are software-defined safety systems operating in open, adversarial environments.

Software Safety in ADAS Systems

ADAS functionality increasingly depends on:

- Software updates
- Sensor fusion algorithms
- Machine learning inference
- Real-time decision-making

This creates **new failure modes**:

- Software regressions introduced via OTA
- Misclassification under rare conditions
- Unintended interactions between features
- Over-reliance by drivers (automation complacency)

Implication:

Safety assurance must evolve from static validation to **continuous, lifecycle- based assurance**.

4.3 AI Safety, Sensor Spoofing & Adversarial Attacks

The Emerging Threat Surface

As ADAS and autonomous functions rely heavily on AI-driven perception and decision-making, they become susceptible to **non-traditional attack vectors**— both accidental and adversarial.

Sensor Spoofing & Environmental Manipulation

Attack vectors include:

- Lidar spoofing using light interference
- Camera deception through altered signage or projections
- Radar interference
- GPS spoofing and jamming

These attacks do not require direct vehicle access and can exploit **environmental vulnerabilities**.

Adversarial AI Attacks

AI models can be:

- Tricked into misclassification
- Degraded through data poisoning
- Rendered unstable through edge-case manipulation

Even non-malicious factors—weather, glare, road degradation—can trigger similar failure modes.

Key Insight:

The distinction between “cyber-attack” and “operational risk” is rapidly collapsing.

Why Traditional Safety Models Are Insufficient

Conventional automotive safety frameworks assume:

- Predictable failure modes
- Deterministic system behavior
- Clear fault isolation

AI-driven systems violate all three assumptions.

Result:

Safety assurance must now incorporate **probabilistic reasoning, adversarial testing, and resilience engineering**.

4.4 Why Cyber-Resilience Matters More Than Autonomy Hype

The industry narrative is shifting—quietly but decisively—from *how autonomous a vehicle is* to *how resilient it is when autonomy degrades*.

Cyber-Resilience Defined

Cyber-resilience refers to a system’s ability to:

- Detect abnormal behavior
- Degrade gracefully
- Maintain safe operation under attack or uncertainty
- Recover without catastrophic failure

This applies equally to:

- ADAS features
- Autonomous subsystems
- OTA pipelines
- AI inference engines

Regulatory & Market Signals

Global regulators increasingly emphasize:

- Software update governance
- Continuous monitoring
- Incident reporting
- Post-deployment accountability

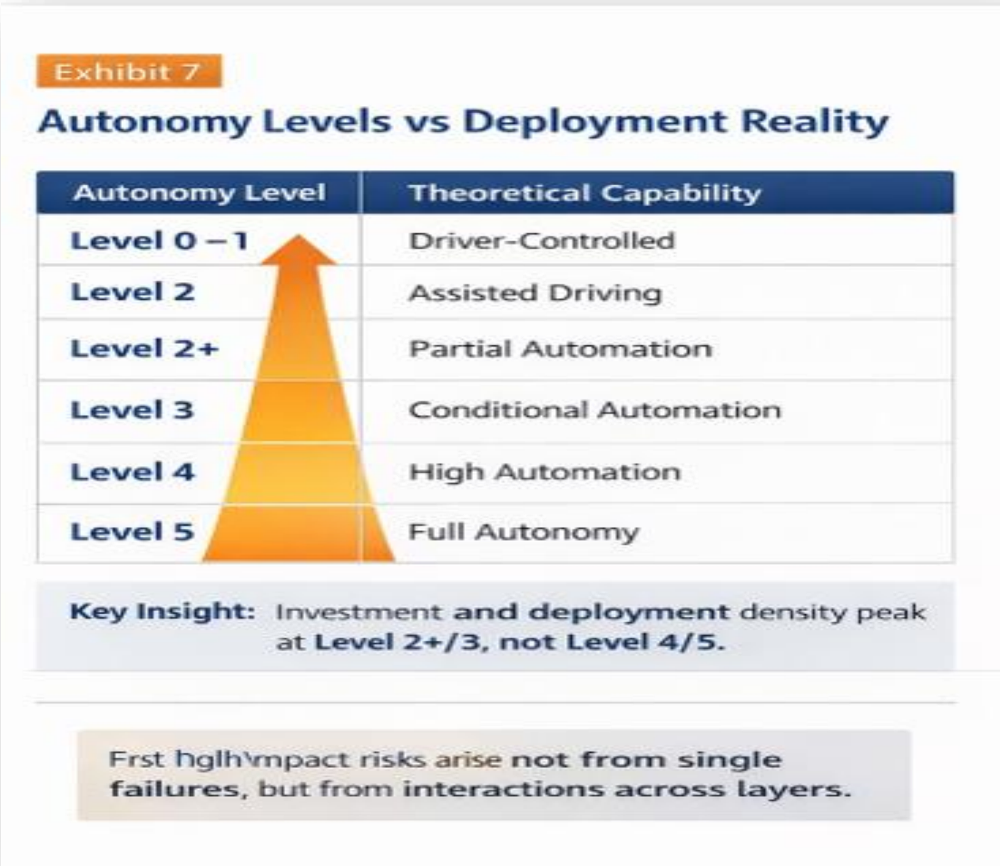
OEMs that cannot demonstrate resilience risk:

- Delayed homologation
- Product recalls
- Brand erosion

Strategic Reality:

In the medium term, **resilient Level 2+/3 systems will deliver more value than fragile higher-level autonomy**.

Exhibit 7: Autonomy Levels vs Deployment Reality



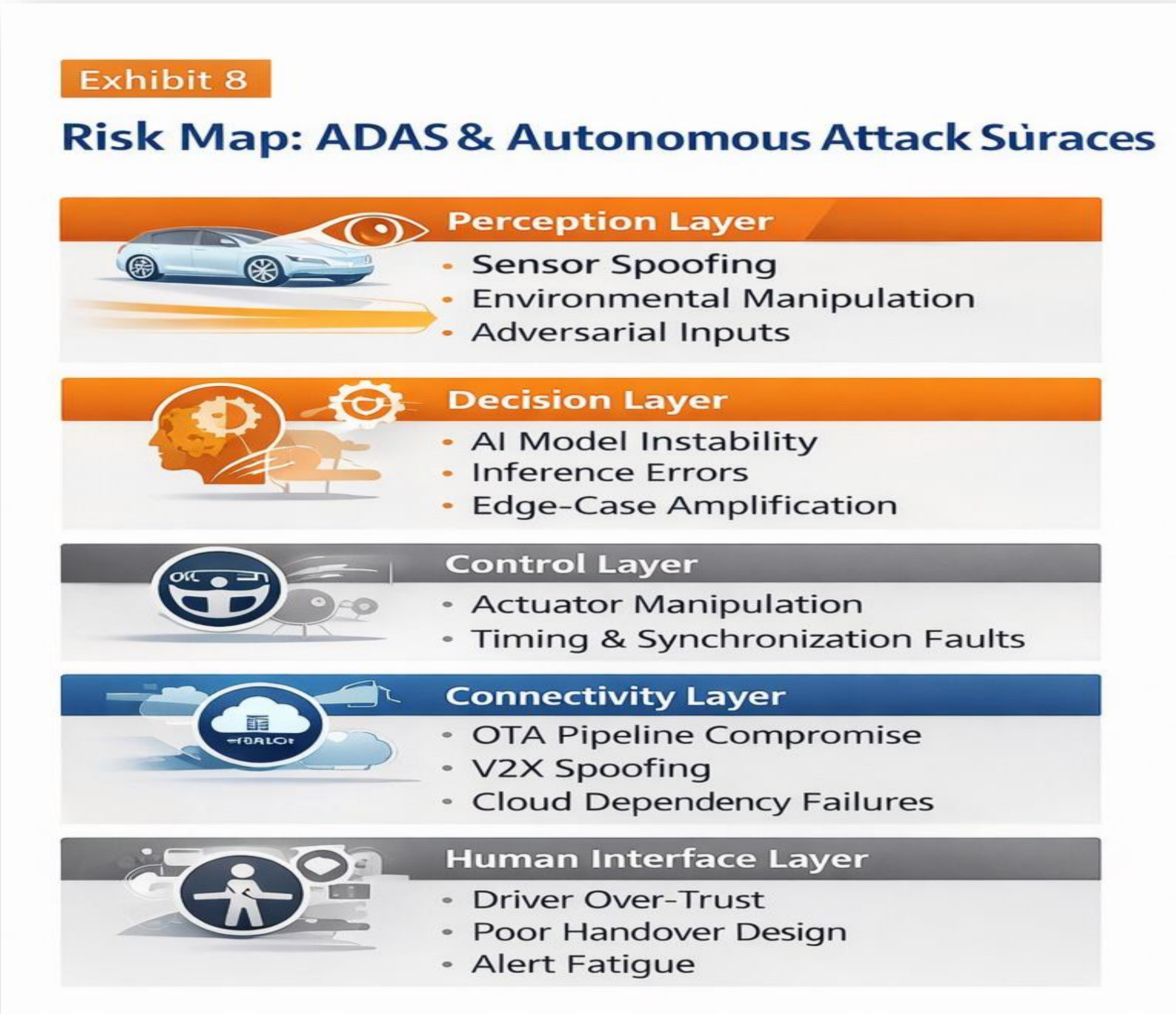
📊 Chart: Nominal Autonomy vs Real-World Deployment

Autonomy Level	Theoretical Capability	Real-World Deployment
Level 0–1	Driver-controlled	Universal
Level 2	Assisted driving	Mass-market
Level 2+	Partial automation	Rapidly expanding
Level 3	Conditional automation	Limited, geo-fenced
Level 4	High automation	Pilot-only
Level 5	Full autonomy	Experimental

Observation:

Investment and deployment density peak at **Level 2+/3**, not Level 4/5.

Exhibit 8: Risk Map – ADAS & Autonomous Attack Surfaces



📈 Risk Map: Key Vulnerability Domains

Perception Layer

- Sensor spoofing
- Environmental manipulation
- Adversarial inputs

Decision Layer

- AI model instability
- Inference errors
- Edge-case amplification

Control Layer

- Actuator manipulation
- Timing and synchronization faults

Connectivity Layer

- OTA pipeline compromise
- V2X spoofing
- Cloud dependency failures

Human Interface Layer

- Driver over-trust
- Poor handover design
- Alert fatigue

Key Insight:

Most high-impact risks arise **not from single failures, but from interactions across layers**.

4.5 Strategic Takeaways

1. **Autonomy is constrained by trust, not ambition**
2. **ADAS is the primary delivery vehicle for intelligence at scale**
3. **AI safety and cyber-resilience are inseparable**
4. **Graceful degradation is as important as peak performance**
5. **Resilience engineering is becoming a competitive differentiator**

These realities reinforce the need for:

- Advanced adversarial testing environments

- AI safety validation frameworks
- Continuous post-deployment monitoring
- Institutional-scale cyber and resilience testbeds

—capabilities that extend beyond individual OEM economics.

This shift—from autonomy as capability to autonomy as resilience—naturally leads to **automotive cybersecurity as a core system discipline**, addressed in the next section.

Section 5
Automotive Cybersecurity & AI Safety: The New Homologation Layer

Why Market Access, Safety, and Trust Are Now Software- and Security-Defined

5.1 Vehicles as National Cyber-Physical Assets

Modern vehicles are no longer isolated mechanical products; they are **mobile, networked cyber-physical systems** that interact continuously with digital infrastructure, cloud platforms, energy grids, and public networks.

A single connected vehicle today may include:

- 100+ ECUs and domain controllers
- Multiple wireless interfaces (Bluetooth, Wi-Fi, cellular, UWB)
- Continuous OTA update pipelines

AI models making real-time safety-critical decisions As a result, vehicles now sit at the intersection of:

- **Public safety**
- **National digital infrastructure**
- **Energy and transport systems**
- **Consumer data and privacy**

Key Insight:

From a regulatory and strategic perspective, connected vehicles increasingly resemble **critical infrastructure assets**, not consumer electronics.

This shift fundamentally changes how governments, regulators, and OEMs must approach cybersecurity—moving from voluntary best practices to **mandatory, auditable assurance**.

5.2 The Global Automotive Cyber Threat Landscape

An Expanding, Multi-Layered Attack Surface

Automotive cyber risk has evolved from isolated infotainment vulnerabilities to **system-wide, safety-critical exposure**. Threat vectors now span the entire vehicle lifecycle—from design and manufacturing to operation and decommissioning.

Wireless & Short-Range Attacks

- Bluetooth and BLE exploitation
- Keyless entry relay attacks
- Wi-Fi and UWB vulnerabilities

Impact: Unauthorized access, theft, privacy breaches

In-Vehicle Network Attacks (CAN, LIN, Ethernet)

- Message injection and spoofing
- Bus-off attacks
- Lateral movement between ECUs

Impact: Loss of control over braking, steering, and safety systems

---

OTA & Firmware Attacks

- Malicious firmware injection
- Man-in-the-middle attacks
- Compromised update servers

Impact: Fleet-wide vulnerabilities, large-scale recalls

V2X & GPS Attacks

- GPS spoofing and jamming
- V2V/V2I message manipulation

Impact: Incorrect situational awareness, traffic safety risks

---

AI-Specific Attacks

- Adversarial inputs to perception systems
- Model poisoning during training or updates
- Inference manipulation in edge AI systems

Impact: Silent failure modes that evade traditional detection

Key Insight:

Automotive cyber threats increasingly exploit interactions across layers, rather than single points of failure.

5.3 Global Regulations & Compliance Mandates

Cybersecurity Has Become a Market-Access Requirement

Over the last five years, cybersecurity has shifted from guidance to **binding regulation** across major automotive markets.

UNECE WP.29 (Cybersecurity & Software Updates)

UNECE WP.29 regulations require OEMs to:

- Implement a Cybersecurity Management System (CSMS)
- Demonstrate risk identification and mitigation
- Monitor threats throughout the vehicle lifecycle
- Manage secure software updates

Implication:

Cybersecurity is now a **precondition for vehicle homologation** in multiple global markets.

ISO/SAE 21434

ISO/SAE 21434 defines:

- Cybersecurity engineering processes
- Threat analysis and risk assessment (TARA)
- Secure development and validation practices

Implication:

Cybersecurity must be embedded into **product development**, not retrofitted post-design.

NHTSA (United States)

NHTSA guidelines emphasize:

- Risk-based cybersecurity approaches
- Incident reporting and disclosure
- Post-deployment monitoring

EU Cyber Resilience Act

The EU Cyber Resilience Act extends cybersecurity obligations to:

- Software components
- OTA update mechanisms
- Long-term support and vulnerability management

Implication:

OEMs and suppliers assume **ongoing liability** for software security over the vehicle's operational life.

5.4 India's Compliance Readiness Gap

A Growing Disconnect Between Capability and Requirement

India's automotive ecosystem has made significant progress in connectivity, electrification, and digital features. However, cybersecurity readiness remains **uneven and fragmented**.

Key Gaps

1. **Fragmented Validation Infrastructure**

   Limited access to shared cyber testing, adversarial simulation, and OTA validation environments.

2. **Late-Stage Security Integration**

   Cybersecurity often addressed during certification rather than design.

3. **Skills Shortage**

   Limited availability of automotive-grade cybersecurity and AI safety engineers.

4. **Supplier Readiness Variance**

   Tier-2 and Tier-3 suppliers often lack cybersecurity engineering maturity.

5. **Export Compliance Risk**

   Increasing risk of delayed homologation and market access restrictions.

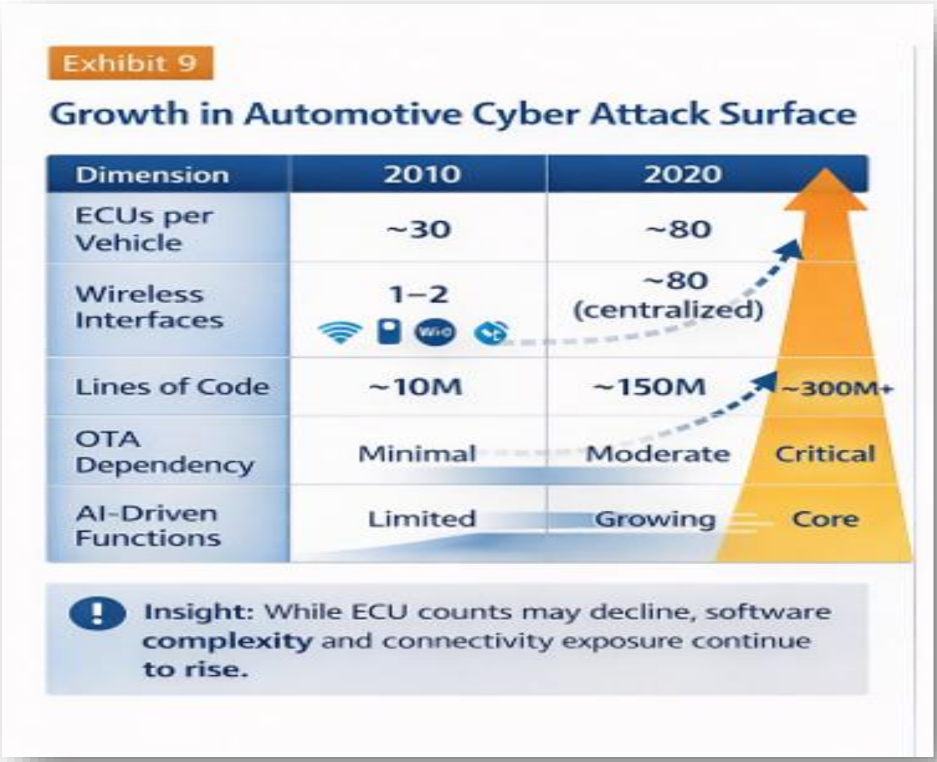
Strategic Risk:

Without coordinated capability development, Indian OEMs risk becoming **technology adopters without assurance ownership**.

Exhibit 9: Automotive Attack Surface Growth

📊 **Chart: Growth in Automotive Cyber Attack Surface (Indicative)**

Dimension	2010	2020	2035 (Projected)
ECUs per Vehicle	30	80	40 (centralized)
Wireless Interfaces	1–2	5–7	8–10
Lines of Code	10M	150M	300M+
OTA Dependency	Minimal	Moderate	Critical
AI-Driven Functions	Limited	Growing	Core



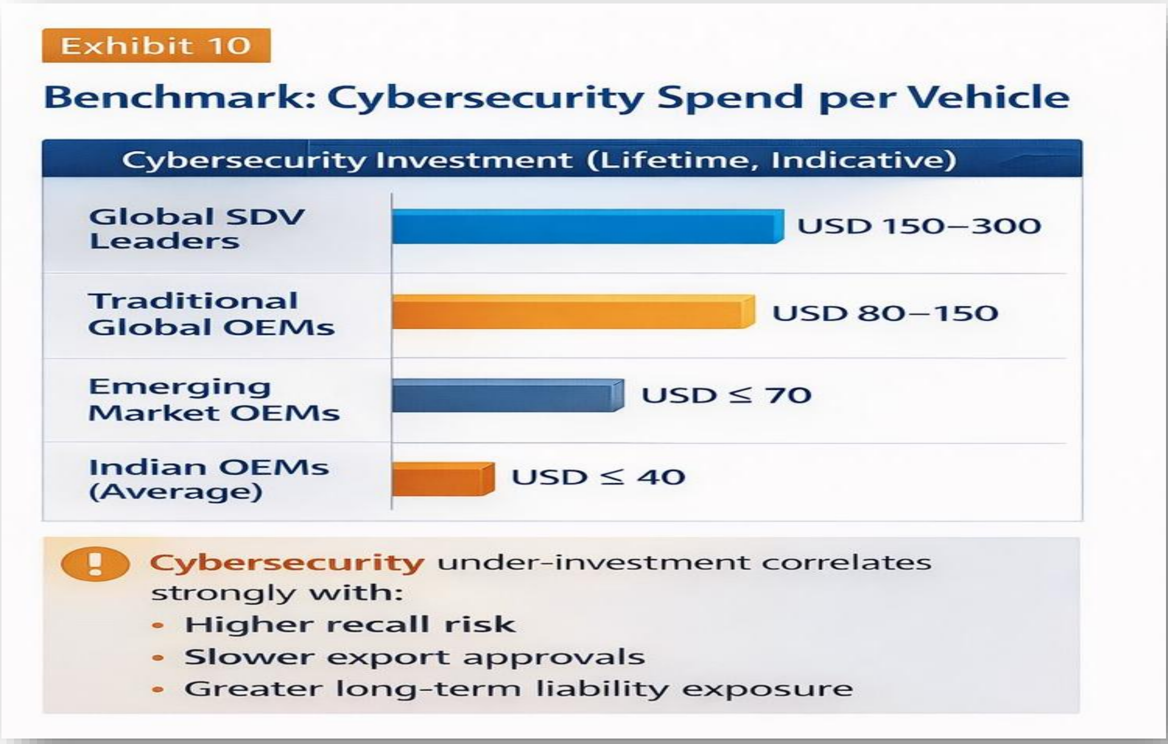
Observation:

While ECU counts may decline, **software complexity and connectivity exposure continue to rise**.

Exhibit 10: Benchmark – Cybersecurity Spend per Vehicle

📈 Cybersecurity Investment (Lifetime, Indicative)

OEM Category	Cybersecurity Spend per Vehicle
Global SDV Leaders	USD 150 – 300
Traditional Global OEMs	USD 80 – 150
Emerging Market OEMs	USD 70
Indian OEMs (Average)	USD 40



Key Insight:

Cybersecurity under-investment correlates strongly with:

- Higher recall risk
- Slower export approvals
- Greater long-term liability exposure

5.5 Strategic Takeaways

1. Automotive cybersecurity is now a homologation layer, not a feature
2. AI safety introduces non-deterministic risk that traditional safety models cannot address
3. Regulatory expectations extend across the full vehicle lifecycle
4. Cybersecurity capability is becoming a source of competitive differentiation
5. Institutional-scale validation and assurance are essential for ecosystem readiness

These dynamics underscore the need for **shared cybersecurity testbeds, AI safety frameworks, certification pathways, and skilled talent pipelines**— capabilities that individual firms struggle to build independently at scale.

As cybersecurity becomes foundational to trust and market access, the focus naturally expands from protecting vehicles to **securing the broader EV, energy, and lifecycle**

ecosystem, addressed in the next section.

Section 6
Electrification, Energy & Circular Economy

From Electric Vehicles to Energy-Integrated, Lifecycle-Aware Mobility Systems

6.1 Beyond EVs: Vehicles as Energy Assets

The global shift toward electrification is often framed narrowly around vehicle propulsion. In reality, the most significant transformation lies beyond drivetrain replacement: **electric vehicles are becoming distributed energy assets** within broader power and sustainability ecosystems.

Leading markets are rapidly redefining the role of vehicles across three dimensions:

- **Energy storage** (mobile batteries at scale)
- **Grid interaction** (vehicle-to-grid and vehicle-to-building)
- **Energy intelligence** (predictive optimization of charging, usage, and degradation)

This reframing positions EVs not merely as consumers of electricity, but as **active participants in energy markets**.

Vehicles in the Energy System

Emerging global models include:

- **Vehicle-to-Grid (V2G):** EVs supplying power back to grids during peak demand
- **Vehicle-to-Home (V2H):** Residential backup and load balancing
- **Fleet-level energy orchestration:** Commercial EV fleets acting as virtual power plants

Impact

- Improved grid stability
- Monetization of idle vehicle capacity
- Integration with renewable energy variability

Key Insight:

The economic value of EVs increasingly extends beyond mobility into **energy arbitrage and grid services**.

6.2 Battery Lifecycle, Second-Life & Recycling

The Battery as the Central Economic and Environmental Asset

The battery is the most valuable, most regulated, and most environmentally sensitive component of an electric vehicle. Its lifecycle—spanning extraction, manufacturing, usage, repurposing, and recycling—defines both the **economics and sustainability** of electrification.

Primary Vehicle Use Phase

During automotive use, battery performance degrades predictably but unevenly, influenced by:

- Charging behavior
- Thermal management
- Duty cycles
- Software controls

Advanced AI-driven battery management systems increasingly optimize this phase to:

- Extend usable life
- Reduce safety risk
- Maximize residual value

Second-Life Applications

When automotive performance falls below mobility thresholds (typically 70– 80% state of health), batteries retain significant functional capacity.

Common second-life applications include:

- Stationary energy storage
- Renewable energy buffering
- Telecom and data-center backup systems

Impact

- Extended asset utilization
- Improved total cost of ownership
- Reduced environmental footprint

Recycling & Material Recovery

At end-of-life, batteries become **strategic material repositories**, containing lithium, cobalt, nickel, copper, and rare-earth elements.

Advanced recycling ecosystems focus on:

- Traceable material recovery
- Closed-loop supply chains
- Reduction of import dependency

Strategic Reality:

Battery recycling is no longer a waste-management problem—it is a **resource security imperative**.

6.3 Global Battery Passport & Traceability Mandates

From Sustainability Claims to Verifiable Proof

Global regulators are rapidly mandating **digital traceability and lifecycle transparency** for batteries and critical components.

EU Battery Regulation & Battery Passport

The European Union's Battery Regulation requires:

- Digital battery passports for industrial and EV batteries
- Disclosure of carbon footprint
- Documentation of material origin and recycled content
- Lifecycle performance and durability data

Implication:

Access to EU markets increasingly depends on **digitally verifiable lifecycle data**, not declarations.

China's Traceability Regime

China mandates:

- End-to-end battery tracking
- OEM responsibility for recycling
- Centralized data reporting platforms

This has enabled China to:

- Build domestic recycling capacity
- Secure material supply chains
- Enforce compliance at scale

Global Direction of Travel

Across jurisdictions, three themes are converging:

1. **Digital passports over paper compliance**
2. **Lifecycle accountability over point-of-sale responsibility**
3. **Technology-enabled enforcement over manual audits**

6.4 India's Opportunity in Lifecycle Trust Platforms

India stands at a critical juncture in the electrification journey.

Structural Advantages

- Rapid EV adoption across two-, three-, and four-wheelers
- Large installed base enabling data-driven lifecycle platforms
- Strong digital public infrastructure
- Growing recycling and energy storage markets

Structural Gaps

- Fragmented lifecycle data
- Limited traceability of batteries and critical components
- Informal recycling ecosystems
- High dependence on imported materials

The Strategic Opportunity

Rather than retrofitting compliance mechanisms, India has the opportunity to **build lifecycle trust platforms natively**, integrating:

- Digital identity for batteries and components
- AI-driven lifecycle intelligence
- Automated EPR and recycling compliance
- Second-life and material recovery marketplaces

Key Insight:

Lifecycle trust platforms can become **strategic national digital infrastructure**, much like payments or identity systems.

Exhibit 11: Battery Lifecycle Flow

📊 Flow Diagram: Battery Lifecycle

Key Features

- Digital identity persists across lifecycle stages
- Performance and health data captured continuously
- Ownership and responsibility transitions recorded
- Recovered materials re-enter supply chain with traceability

Observation:

Value maximization depends on **continuous data and trust across transitions**, not isolated lifecycle stages.

Exhibit 12: Benchmark – Recycling Readiness

Recycling & Circular Economy Readiness (Indicative)

Dimension	EU	China	India
Battery Passport Mandate	Advanced	Advanced	Emerging
Digital Traceability	High	High	Low–Medium
Formal Recycling Capacity	High	High	Emerging
Second-Life Integration	Moderate	High	Limited
Regulatory Enforcement	Strong	Strong	Developing

Key Insight:

India's recycling readiness lags leading markets—but the gap is **structural, not technological**, and can be closed through platform-led approaches.

6.5 Strategic Takeaways

1. **Electrification is evolving into energy-system integration**
2. **Battery lifecycle management defines EV economics**
3. **Global markets are moving toward mandatory digital traceability**
4. **Recycling and second-life are strategic value pools**
5. **Lifecycle trust platforms offer India a leapfrogging opportunity**

These dynamics position electrification not merely as an automotive transition, but as a **systems transformation spanning mobility, energy, sustainability, and digital infrastructure**.

As vehicles become software-defined, AI-driven, cyber-secure, and energy- integrated assets, the question becomes not *what technologies exist*, but **how ecosystems organize to deploy them at scale**—the focus of the next section on India's automotive ecosystem and institutional readiness.

Section 7
India’s Automotive Ecosystem: Current State Assessment

Strong in Scale, Fragmented in Systems

7.1 OEMs, Tier-1s, Startups & MSMEs

India’s automotive ecosystem is one of the largest and most diverse globally, spanning high-volume OEMs, globally integrated Tier-1 suppliers, a rapidly expanding startup landscape, and a vast MSME base. Each segment exhibits distinct strengths—yet the ecosystem as a whole remains **structurally fragmented**.

Original Equipment Manufacturers (OEMs)

Strengths

- Strong manufacturing scale and cost competitiveness
- Deep understanding of price-sensitive markets
- Rapid execution capability in incremental product innovation

Constraints

- Limited ownership of core SDV, AI, and cybersecurity architectures
- Heavy dependence on external software platforms
- R&D portfolios skewed toward hardware and integration rather than system design

Assessment:

Indian OEMs are effective **product integrators**, but are not yet system architects in the SDV era.

Tier-1 & Tier-2 Suppliers

Strengths

- Global delivery capabilities
- Strong process discipline and quality systems
- Growing embedded software competence

Constraints

- Revenue models still dominated by hardware BOM
- Limited pricing power in software-enabled subsystems
- Uneven cybersecurity and OTA readiness across the supply base

Assessment:

Suppliers face a strategic inflection: evolve into **software-defined subsystem providers** or risk commoditization.

Startups & New-Age Mobility Players

Strengths

- High innovation velocity
- Strong capabilities in AI, data, EV subsystems, and digital platforms
- Willingness to adopt SDV-native architectures

Constraints

- Limited access to validation, testing, and certification infrastructure.
- Difficulty integrating with OEM production cycle
- Fragmented standards and compliance pathways

Assessment:

Indian startups are **innovation-rich but scale-constrained**, often stalling at the pilot stage.

MSMEs

Strengths

- Cost efficiency
- Manufacturing flexibility
- Deep participation across the supply chain

Constraints

- Minimal exposure to software, AI, and cybersecurity requirements
- Limited capital for technology transition
- High vulnerability to regulatory and export compliance shifts

Assessment:

Without ecosystem support, MSMEs risk being **structurally excluded** from future automotive value chains.

R&D, Talent & Infrastructure Gaps

Despite India's engineering depth, the automotive ecosystem exhibits **systemic gaps** in how R&D, talent, and infrastructure are organized.

R&D Structure

- R&D spend as a percentage of revenue remains significantly below global SDV leaders
- Research efforts are distributed across firms with limited shared platforms
- Weak translation from academic research to production-grade systems

Key Gap:

India lacks **shared, pre-competitive automotive technology platforms** that de- risk innovation at scale

Talent Availability

India produces large volumes of engineers, but the **talent mix is misaligned** with future automotive needs. High demand, limited supply in:

- SDV architecture design
- Automotive AI and edge inference
- Cybersecurity engineering
- AI safety and validation

Key Gap:

The ecosystem lacks **structured talent pipelines aligned to automotive system roles**, rather than generic IT skills.

Infrastructure & Validation

Critical gaps exist in:

- Automotive cyber ranges
- AI safety and adversarial testing environments
- OTA and lifecycle validation platforms
- Battery lifecycle and recycling testbeds

Key Gap:

Validation and assurance infrastructure is **fragmented, firm-specific, or unavailable at scale**.

7.2 Fragmentation vs Platform Thinking

The Core Structural Challenge

India's automotive ecosystem is not constrained by lack of capability—it is constrained by **lack of coordination and shared systems**.

Today's operating model:

- OEM-specific architectures
- Supplier-specific toolchains
- Startup-specific pilots
- Regulator-specific compliance interpretations

This fragmentation results in:

- Duplication of effort
- Slow adoption of global standards
- High integration costs
- Inconsistent quality and security outcomes

Global Contrast

Leading automotive ecosystems operate on **platform logic**, characterized by:

- Shared reference architectures
- Common validation and certification layers
- Institutional coordination between industry, academia, and regulators
- Talent pipelines aligned to system needs

Key Insight:

Platform thinking enables **ecosystem-level acceleration**, while fragmentation enforces firm-level constraints.

From Vendor-Centric Pilots to Ecosystem Platforms

As automotive systems grow increasingly software-intensive, the limitations of vendor-centric pilot projects become more pronounced. While individual platforms and tools can demonstrate technical capability, their true value is realized only when integrated into validated, standards-aligned system architectures that span the full vehicle lifecycle. Institutional platforms bridge this gap by enabling shared reference zones for operating systems, middleware, embedded software, AI workloads, and cybersecurity controls—without privileging any single vendor.

Such platforms allow multiple technology providers to coexist, interoperate, and evolve within a governed framework, thereby reducing duplication, accelerating OEM adoption, and improving compliance readiness. By anchoring these platforms within a neutral institutional context, CAAR enables a transition from fragmented experimentation to coordinated, ecosystem-wide progress in advanced automotive systems.

"A conceptual illustration of CAAR's role as an institutional anchor within the software-defined vehicle ecosystem is provided in Annexure A."

Exhibit 13: Heat Map – India vs Global Automotive Capabilities

Exhibit 13

Heat Map – India vs Global Automotive Capabilities

Comparative Capability Assessment (Indicative)

Capability Dimension	Global Leaders	India
SDV Architecture Ownership	High	Low-Medium
Automotive AI Maturity	High	Medium
Cybersecurity & AI Safety	High	Low
OTA & Lifecycle Management	High	Medium
Battery Passport & Traceability	High	Emerging
Recycling & Circular Economy	High	Emerging
R&D Intensity	High	Low
Talent Depth (System Roles)	High	Low
Validation Infrastructure	High	Medium
Standards Participation	Low	Low

Overall Assessment: **India** demonstrates **strong** execution **capability** but limited system-level ownership across future-defining dimensions.

Comparative Capability Assessment (Indicative)

Capability Dimension	Global Leaders	India
SDV Architecture Ownership	High	Low–Medium
Automotive AI Maturity	High	Medium
Cybersecurity & AI Safety	High	Low

OTA & Lifecycle Management	High	Medium
Battery Passport & Traceability	High	Emerging
Recycling & Circular Economy	High	Emerging
R&D Intensity	High	Low

Overall Assessment:

India demonstrates **strong execution capability** but **limited system-level ownership** across future-defining dimensions.

7.3 Strategic Diagnosis

1. India's automotive ecosystem is **broad but shallow** in next-generation system capabilities
2. Fragmentation, not innovation, is the primary bottleneck
3. Individual firms cannot economically build all required future capabilities independently
4. Shared platforms and institutional orchestration are missing links This

diagnosis frames a critical transition point:

The future competitiveness of India's automotive sector depends less on incremental capability building—and more on how capabilities are integrated, validated, and scaled across the ecosystem.

The assessment above raises an unavoidable question:

Who will provide the neutral platforms, shared infrastructure, system validation, and talent orchestration that the ecosystem requires—but no single firm can efficiently deliver?

Section 8 addresses that question directly by examining the case for **CAAR as India's Automotive Technology Nerve Center**.

Capability Dimension	Global Leaders	India
Talent Depth (System Roles)	High	Medium
Validation Infrastructure	High	Low
Standards Participation	High	Low

Section 8
The Case for CAAR as India's Automotive Technology Nerve Center

Why Future Automotive Leadership Is Institutional—Not Individual

8.1 Global Analogues: How Automotive Leadership Is Actually Built

A consistent pattern emerges when examining countries that have sustained leadership across automotive technology transitions: **no nation has succeeded through market forces alone**.

Instead, leadership is anchored by **institutional platforms** that sit between industry, academia, and the state—providing continuity, neutrality, and system- level capability.

Germany: Fraunhofer Institutes

Germany's automotive strength is underpinned not only by OEMs, but by the **Fraunhofer Society**, a network of applied research institutes deeply embedded in industrial value chains.

Defining Characteristics

- Mission-driven applied research
- Pre-competitive collaboration with OEMs and suppliers
- Strong IP creation and transfer mechanisms
- Deep integration with standards bodies

Impact

- Continuous translation of research into production systems
- Reduced innovation risk for industry
- Sustained leadership across multiple technology cycles

Key Insight:

Fraunhofer acts as a **technology stabilizer and accelerator** for the German automotive ecosystem.

United States: NHTSA + National Laboratories

In the United States, automotive leadership is reinforced by a **distributed institutional model**, combining regulatory authority and deep technical capability.

Key Components

- NHTSA defining safety and cybersecurity expectations
- National Labs providing advanced testing, simulation, and validation
- Strong academia–industry pipelines

Impact

- Early integration of safety, cybersecurity, and autonomy considerations
- Clear pathways from experimental technology to regulatory acceptance

Key Insight:

The U.S. model demonstrates that **regulation and innovation scale best when institutionally co-designed**.

China: State-Backed Automotive & Cybersecurity Labs

China has taken a more centralized approach, establishing **state-backed laboratories** focused on EVs, batteries, cybersecurity, and autonomous systems.

Defining Characteristics

- Mandatory technology validation regimes
- Centralized data and traceability platforms
- Tight coupling between industrial policy and technical enforcement

Impact

- Rapid scaling of EV and battery ecosystems
- Accelerated domestic capability development
- Reduced dependence on foreign validation infrastructure

Key Insight:

China's success highlights the power of **institutional scale and enforcement** in shaping markets.

Global Pattern

Across these models, one conclusion is clear:

Sustained automotive leadership requires institutions that provide continuity, trust, validation, and system-level integration—beyond what individual firms can deliver.

8.2 CAAR's Unique Positioning

India's automotive ecosystem lacks a comparable institutional anchor today. However, **CAAR @ IIT Madras is uniquely positioned to assume this role**, based on three structural advantages.

The IIT Madras Ecosystem

IIT Madras offers:

- Global credibility in engineering and applied research
- Cross-disciplinary depth spanning AI, systems engineering, energy, and cybersecurity
- Proven ability to translate research into real-world impact

Why this matters:

Automotive transformation is no longer a single-discipline problem—it requires **systems thinking across software, hardware, energy, and policy domains**.

Industry Credibility

CAAR has been built with **direct industry engagement**, not as an isolated academic initiative.

Key attributes include:

- Deep familiarity with OEM and supplier constraints
- Alignment with production, validation, and compliance realities
- Ability to operate in pre-competitive and competitive contexts

Why this matters:

Trust is a prerequisite for ecosystem orchestration. CAAR's credibility enables collaboration that pure regulatory or academic bodies cannot achieve.

Policy Proximity (Without Policy Dependence)

CAAR operates close enough to policymakers to:

- Understand regulatory trajectories
- Anticipate compliance requirements
- Inform standards alignment

Yet remains sufficiently independent to:

- Maintain technical neutrality

- Avoid policy capture
- Retain global credibility

Why this matters:

Effective nerve centers must **bridge policy and industry without becoming extensions of either**.

8.3 From Centre of Excellence to Ecosystem Orchestrator

Why the Traditional CoE Model Is Insufficient

Conventional Centres of Excellence typically focus on:

- Research outputs
- Pilot projects
- Skill development in isolation

While valuable, this model does not address:

- System-level integration
- Validation at industry scale
- Long-term lifecycle governance
- Standards participation

The Orchestrator Model

An automotive technology nerve center performs four interconnected functions:

1. **Reference Architecture & Validation Authority**

   Providing shared SDV, AI, cybersecurity, and lifecycle reference frameworks.

2. **Assurance & Certification Enablement**

   Enabling compliance with global regulations through testing, simulation, and auditability.

3. **Ecosystem Integration**

   Aligning OEMs, suppliers, startups, academia, and regulators on common platforms.

4. **Capability & Talent Orchestration**

Building system-level skills pipelines aligned to real industry roles.

Key Insight:

The orchestrator does not replace firms—it **multiplies their effectiveness**.

Exhibit 14: Comparative View – Global Automotive CoEs vs CAAR

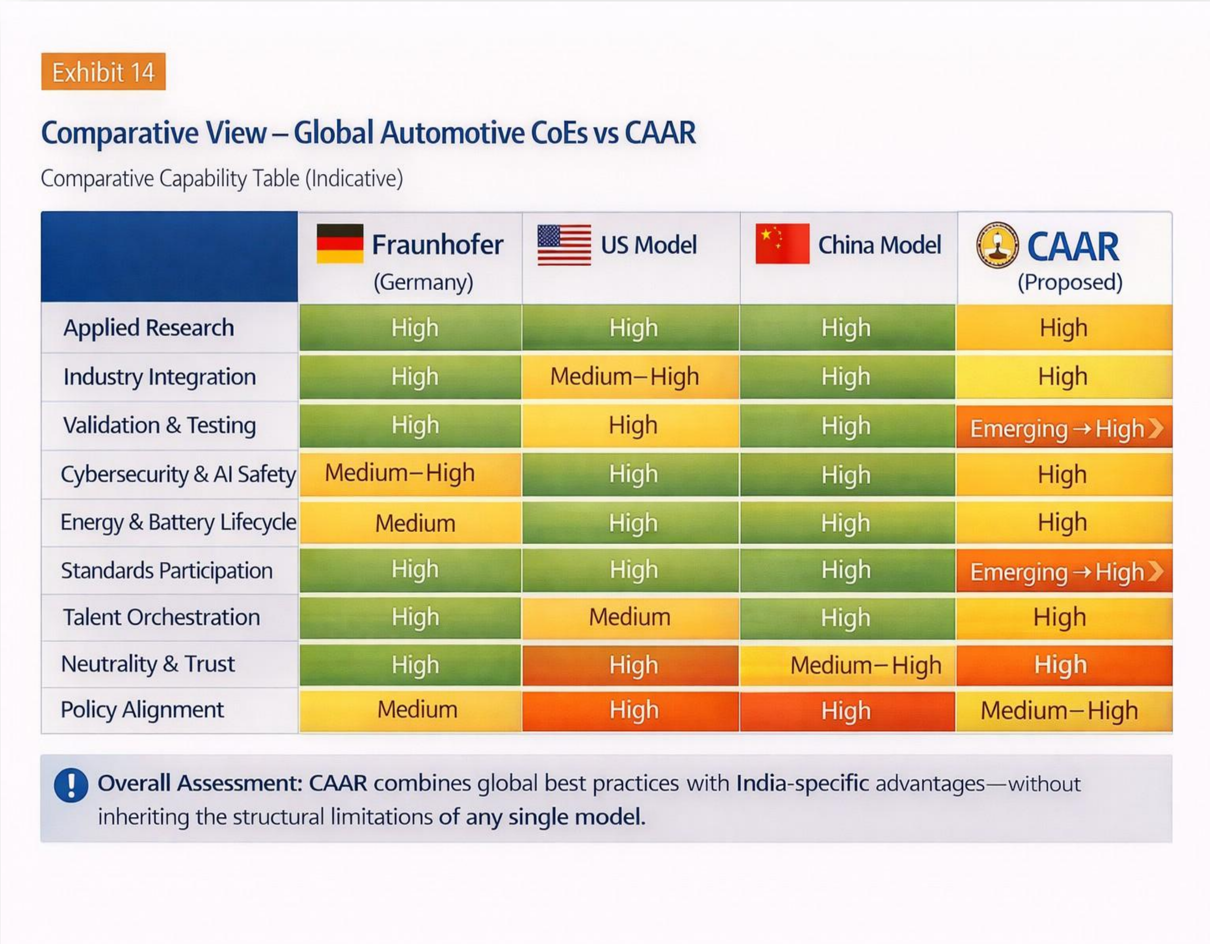


Exhibit 14

Comparative View – Global Automotive CoEs vs CAAR

Comparative Capability Table (Indicative)

	Fraunhofer (Germany)	US Model	China Model	CAAR (Proposed)
Applied Research	High	High	High	High
Industry Integration	High	Medium–High	High	High
Validation & Testing	High	High	High	Emerging → High
Cybersecurity & AI Safety	Medium–High	High	High	High
Energy & Battery Lifecycle	Medium	High	High	High
Standards Participation	High	High	High	Emerging → High
Talent Orchestration	High	Medium	High	High
Neutrality & Trust	High	High	Medium–High	High
Policy Alignment	Medium	High	High	Medium–High

Overall Assessment: CAAR combines global best practices with India-specific advantages—without inheriting the structural limitations of any single model.

Comparative Capability Table (Indicative)

Dimension	Fraunhofer (Germany)	US Model	China Model	CAAR (Proposed)
Applied Research	High	High	High	High
Industry Integration	High	Medium–High	High	High
Validation & Testing	High	High	High	Emerging → High
Cybersecurity & AI Safety	Medium–High	High	High	High
Energy & Battery Lifecycle	Medium	Medium	High	High

Standards Participation	High	High	Medium	Emerging → High
Talent Orchestration	High	High	Medium	High
Neutrality & Trust	High	Medium	Medium	High
Policy Alignment	Medium	High	High	Medium–High

Overall Assessment:

CAAR combines **global best practices** with India-specific advantages—without inheriting the structural limitations of any single model.

8.4 Strategic Implication

Sections 1–7 established that:

- Automotive value is shifting toward software, AI, cybersecurity, and lifecycle systems
- India's ecosystem is capable but fragmented•Individual firms cannot economically build all required future capabilities alone

Section 8 demonstrates that:

The absence of a neutral, technically credible, system-level orchestrator is the single largest structural gap in India's automotive ecosystem.

CAAR is uniquely positioned to fill this gap—not as an advisory body, regulator, or vendor, but as **India's Automotive Technology Nerve Center**.

Next section defines how this role translates into concrete strategic pillars, programs, and outcomes over the next decade.

Section 9
CAAR Strategic Pillars (2026–2035)

From Institutional Credibility to Systemic National Impact

9.1 Certification & Compliance Authority

Embedding Trust, Safety, and Market Access into India's Automotive Ecosystem

As automotive systems become software-defined, AI-driven, and lifecycle- regulated, **certification and compliance are no longer peripheral activities**.
They are emerging as **primary enablers of global market access, brand trust, and regulatory acceptance**.

Today, the Certification process is long and drawn (with a usually long queue time) and any failure at the validation results in significant delays to the certification and hence, the component seeing the light of the day. Here, CAAR's role would be to provide the **development and integration verification tests,** assisting in being certification-ready, and thus, reducing any failures on the final certification process.

In the next stage, CAAR itself could slip into the role as a **neutral, technically authoritative certification and validation anchor**, enabling Indian OEMs and suppliers to meet global requirements efficiently and consistently.

Automotive Cybersecurity Certification

CAAR will enable:

- Cybersecurity Management System (CSMS) validation.
- Threat Analysis & Risk Assessment (TARA) assurance
- Continuous post-deployment monitoring frameworks

Outcome

- Reduced homologation delays
- Improved export readiness
- Lower recall and liability exposure

SDV & OTA Compliance Labs

SDV architectures and OTA pipelines require continuous validation across:

- Software updates

- Configuration management
- Regression and safety assurance

CAAR will establish **SDV and OTA compliance labs** that simulate real-world operational and adversarial conditions.

Outcome

- Faster SDV deployment cycles
- Safer OTA rollouts
- Reduced field failures

Battery & Component Passport Validation

As digital traceability becomes mandatory globally, CAAR will support:

- Battery passport verification
- Component lifecycle traceability
- Compliance with sustainability and recycling mandates

Outcome

- Seamless access to regulated global markets
- Digitally verifiable lifecycle compliance

9.2 Patented Product & IP Development

From Knowledge Generation to Platform Ownership

To avoid structural dependence on imported platforms, India must develop **indigenous, globally relevant automotive IP**. CAAR will focus on **platform- level IP creation**, not point solutions.

Reference SDV Architectures

CAAR will develop and maintain:

- Open, modular SDV reference architectures
- Security- and OTA-by-design frameworks
- Interoperability standards for OEM and supplier adoption

Outcome

- Reduced SDV development risk
- Faster time-to-market

- Shared architectural foundation across the ecosystem

Automotive Cyber Toolchains

Cybersecurity assurance requires specialized tooling for:

- Embedded systems
- Vehicle networks
- OTA pipelines
- AI model validation

CAAR will incubate **automotive-grade cyber toolchains** with patentable IP.

Outcome

- Reduced dependence on foreign tools
- Exportable cybersecurity platforms

AI-Driven Manufacturing Platforms

CAAR will develop AI platforms for:

- Quality inspection
- Predictive maintenance
- Yield optimization
- Autonomous process control

Outcome

- Higher manufacturing productivity
- Lower defect and recall rates
- Competitive differentiation for Indian plants

9.3 AI-Native Manufacturing Excellence

Reimagining Manufacturing as a Learning System

Manufacturing competitiveness in the next decade will be defined by **AI-native plants**, where intelligence is embedded across design, production, and operations.

Digital Twins for Plants

CAAR will enable:

- End-to-end digital twins of manufacturing lines

- Real-time simulation and optimization
- Virtual commissioning and change validation

Outcome

- Faster plant ramp-ups
- Lower capex risk
- Improved operational resilience

AI Quality & Yield Optimization

AI-driven systems will:

- Detect defects earlier
- Identify root causes autonomously
- Optimize yield in real time

Outcome

- Predictive, not reactive, quality control
- Lower scrap and rework

Autonomous Factories

In advanced stages, CAAR-supported plants will move toward:

- Self-optimizing processes
- Minimal human intervention in repetitive control loops
- Human oversight focused on system design and improvement

Outcome

- Globally competitive manufacturing benchmarks

9.4 National Training & Skilling at Scale

Building System-Level Talent, Not Isolated Skills

India's future automotive competitiveness depends on **system architects and assurance engineers**, not just developers or operators.

CAAR will function as a **national skilling and certification engine**, aligned with real industry roles.

Automotive Software Engineers

- SDV architecture
- Vehicle OS and middleware
- OTA lifecycle management

Cybersecurity Specialists

- Automotive threat modeling
- Embedded and OTA security
- AI safety and adversarial testing

EV & Battery Technologists

- Battery management systems
- Lifecycle analytics
- Recycling and second-life integration

Outcome

- Industry-ready talent at scale
- Reduced skill mismatch
- Stronger employer confidence

9.5 Industry–University–Government Collaboration

From Bilateral Engagements to Living Ecosystems

CAAR's orchestration role extends beyond labs and certifications into **continuous ecosystem integration**.

Living Labs

CAAR will operate living labs where:

- OEMs, suppliers, startups, and researchers collaborate
- Technologies are tested in near-production environments

Outcome

- Faster innovation-to-production cycles

Shared Testbeds

Shared infrastructure for:

- Cybersecurity and AI safety testing

- SDV and OTA validation
- Battery lifecycle simulation

Outcome

- Lower entry barriers for startups and MSMEs
- Consistent quality and assurance

[[

Global Joint Research Programs

CAAR will anchor:

- International research collaborations
- Standards development initiatives
- Cross-border validation programs

Outcome

- Global credibility
- Indian participation in setting—not just adopting—standards

---

Exhibit 15: CAAR Maturity Model (2026–2035)

📈 Maturity Model: CAAR Evolution

Phase 1 Research Hub (2026-2027)

- Advanced research and pilot programs
- Initial industry engagement

Phase 2 Platform Provider (2028-2031)

- Shared reference architectures
- Validation and certification services
- Scaled training programs

Phase 3 National Authority (2032-2035)

- De facto standards anchor
- Global certification recognition
- Exportable platforms and IP

Key Insight:

CAAR's evolution mirrors that of successful global institutions—**from knowledge creation to ecosystem authority**.

9.6 Strategic Implication

By 2035, CAAR's strategic pillars position it to:

- De-risk innovation for industry
- Enable global compliance at scale
- Build sovereign technology capability
- Anchor India's transition to software-defined, secure, and sustainable mobility

This sets the stage for the final sections, which quantify **roadmaps, governance models, and measurable national outcomes**.

Below is a **full, flagship-grade draft of Section 10**, written in **Big-4 workforce transformation style**—forward-looking, system-oriented, and tightly aligned to Sections 1–9.

This section positions **talent and certification as strategic infrastructure**, not HR programs.

Section 10
Workforce Transformation & Certification Framework

Building System Architects for a Software-Defined Automotive Era

10.1 Future Automotive Roles

The transformation of the automotive industry into a software-defined, AI- native, cyber-secure, and energy-integrated system is fundamentally a **workforce transformation challenge**.

Traditional role definitions—mechanical engineer, electrical engineer, production supervisor—are no longer sufficient to design, build, validate, and operate next-generation vehicles.

Instead, the industry is converging toward **system-level roles** that combine software, hardware, data, safety, and lifecycle accountability.

Emerging Role Clusters

1. **SDV & Automotive Software Roles**

- SDV System Architect
- Vehicle OS & Middleware Engineer
- OTA Lifecycle Manager
- Embedded Software Integration Lead

Core Competencies

- Centralized compute architectures
- Software–hardware decoupling
- Continuous deployment and validation

Automotive AI & Intelligence Roles

- Automotive AI Engineer (Edge + Cloud)
- ADAS & Perception Specialist
- Digital Twin & Simulation Engineer
- AI Validation & Assurance Engineer

Core Competencies

- Model lifecycle management
- Data pipelines and inference optimization
- AI safety and explainability

---

2. **Cybersecurity & AI Safety Roles**

- Automotive Cybersecurity Engineer
- Threat Modeling & TARA Specialist
- OTA & Supply-Chain Security Lead
- Adversarial AI Testing Specialist

Core Competencies

- Embedded security
- Secure update pipelines
- Cyber-physical risk management

---

3. **EV, Battery & Energy System Roles**

- Battery Management Systems Engineer Energy Systems & V2G Specialist
- Battery Lifecycle & Recycling Technologist
- Sustainability & Compliance Engineer

Core Competencies

- Battery degradation analytics
- Energy integration
- Lifecycle traceability

---

4. **Manufacturing Intelligence Roles**

- AI Manufacturing Engineer
- Digital Twin & Smart Factory Architect
- Autonomous Quality Systems Lead

Core Competencies

- AI-driven quality control
- Predictive operations

- Factory-scale system optimization

Key Insight:

The future automotive workforce is defined less by discipline and more by **system responsibility across the vehicle lifecycle**.

10.2 National Certification Stack

From Fragmented Training to Trusted, Industry-Grade Credentials

As automotive roles become more complex and safety-critical, **informal or generic certifications are no longer sufficient**. Industry requires **trusted, role- aligned, and globally recognized credentials**.

CAAR's approach is to enable a **National Automotive Certification Stack**, structured across three layers.

Layer 1: Foundation Certifications

(Entry-level and transition roles)

- Automotive Software Fundamentals
- EV & Battery Basics
- Cybersecurity Awareness for Automotive Systems

Purpose

- Enable reskilling of existing workforce
- Create a common baseline across OEMs, suppliers, and MSMEs

Layer 2: Professional Certifications

(Role-specific, industry-aligned)

- Certified SDV Engineer
- Certified Automotive AI Engineer
- Certified Automotive Cybersecurity Specialist
- Certified EV & Battery Technologist

Purpose

- Validate role readiness
- Reduce onboarding and integration risk for employers

Layer 3: Advanced & Specialist Certifications

(System-level and leadership roles)

- SDV System Architect
- AI Safety & Assurance Lead
- Automotive Cyber Resilience Architect
- Digital Manufacturing Systems Architect

Purpose

- Build system owners and technical leaders
- Support global credibility and export readiness

Design Principle:

Certifications are **outcome- and capability-based**, not attendance-based.

10.3 Global Accreditation Alignment

Ensuring Global Mobility, Trust, and Recognition

For certifications to deliver long-term value, they must align with **global standards and accreditation frameworks**, not operate in isolation.

Alignment with Global Frameworks

The certification stack is designed to align with:

- ISO / IEC standards
- UNECE WP.29 cybersecurity expectations
- ISO/SAE 21434 role requirements
- Functional safety (AIS189, 190) and AI governance frameworks

---

International Recognition Pathways

CAAR-enabled certifications can be:

- Co-branded with international institutions
- Benchmarked against global professional standards
- Accepted by multinational OEMs and suppliers

Outcome

- Enhanced global employability of Indian professionals
- Increased confidence of global OEMs in Indian talent pools

Continuous Learning & Re-Certification

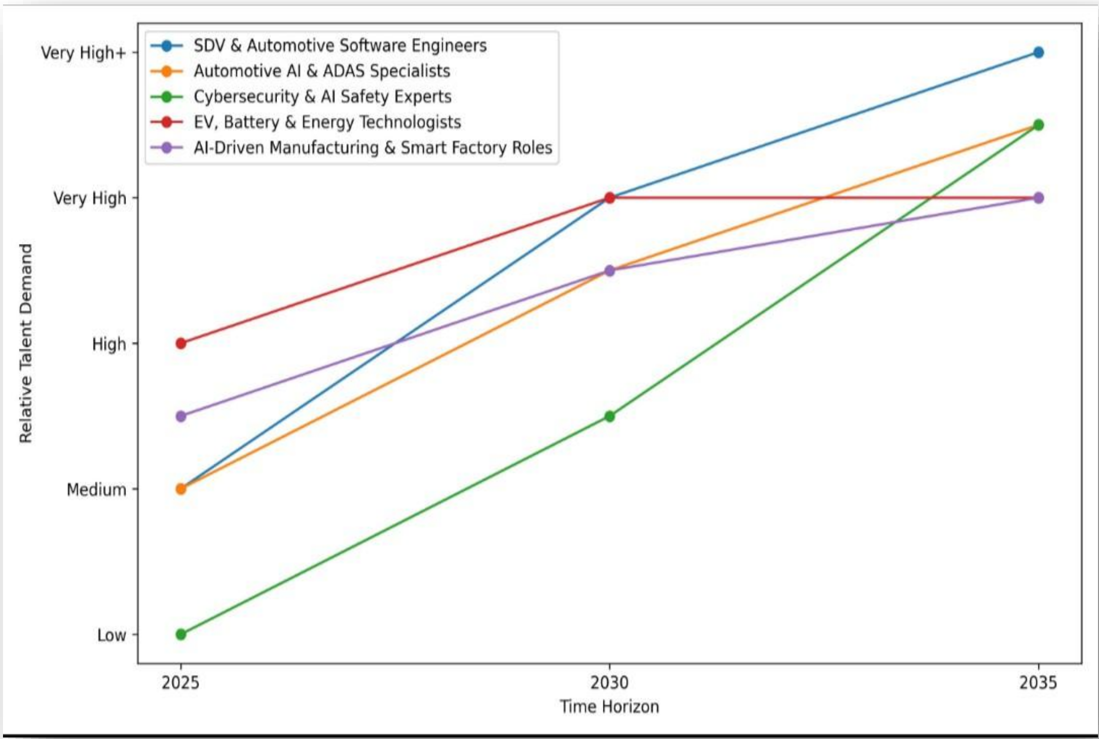
Given rapid technology evolution:

- Certifications will include **periodic renewal**
- Continuous learning credits will be mandated
- Updates will reflect regulatory and technology shifts

Key Insight:

Automotive competence is no longer static—it must be **continuously validated**.

Exhibit 16: Talent Demand Projection till 2035



📊 **Chart: Automotive Talent Demand Growth (Indicative)**

Role Category	2025	2030	2035
SDV & Automotive Software	Medium	High	Very High
Automotive AI & ADAS	Medium	High	Very High
Cybersecurity & AI Safety	Low	Medium	High
EV, Battery & Energy Systems	Medium	High	High
AI-Driven Manufacturing	Medium	High	High

Key Observations

- Demand growth is strongest in **software, AI, and cybersecurity roles**
- Cybersecurity and AI safety show the steepest growth curve
- Manufacturing roles shift from execution to intelligence and system oversight

10.4 Strategic Takeaways

1. **Workforce transformation is the limiting factor in automotive competitiveness**
2. **Future roles are system-oriented, not discipline-bound**
3. **Trusted certification reduces industry risk and accelerates adoption**
4. **Global alignment is essential for talent mobility and export readiness**
5. **Talent infrastructure must scale in parallel with technology infrastructure**

This workforce framework positions talent not as a support function, but as a strategic enabler of India's automotive transformation.

With talent, platforms, and institutional capability defined, the final step is to translate ambition into **timelines, milestones, and measurable outcomes**—the focus of the next section.

Section 11
10-Year Roadmap & Milestones (2026–2035)

Translating Institutional Ambition into Measurable National Impact

The transformation of CAAR from a Centre of Excellence to India's Automotive Technology Nerve Center requires **sequenced capability build-out**, disciplined execution, and transparent measurement. The roadmap below aligns technology maturation with ecosystem adoption and global credibility.

11.1 Roadmap Overview

The roadmap is structured across **three deliberate phases**, each with distinct objectives, investments, and success metrics:

- **Phase 1 (2026–2027): Foundation & Labs**
- **Phase 2 (2028–2031): National Adoption**
- **Phase 3 (2032–2035): Global Leadership**

Each phase builds cumulatively—capabilities established early become platforms for scale and authority later.

Phase 1: Foundation & Labs (2026–2027)

Building the Core Capability Stack

Strategic Objective

Establish CAAR's technical credibility and operational backbone across SDV, AI, cybersecurity, manufacturing intelligence, and lifecycle systems.

Key Initiatives

- Commission SDV, OTA, and automotive cybersecurity labs
- Establish AI manufacturing and digital twin pilot platforms
- Launch battery lifecycle, passport, and traceability testbeds
- Initiate foundational workforce certification programs
- Formalize industry partnerships and advisory councils

Milestones

- First reference SDV architectures released
- Cybersecurity and OTA validation pilots operational

- Initial cohort of certified automotive software and cybersecurity professionals
- Early IP filings and platform prototypes

Outcome

CAAR recognized as a **credible technical authority** and preferred partner for advanced automotive experimentation.

Phase 2: National Adoption (2028–2031)

Scaling Platforms Across the Ecosystem

Strategic Objective

Move from pilots to **industry-wide adoption**, embedding CAAR platforms into OEM, supplier, startup, and skilling ecosystems.

Key Initiatives

- Scale certification and validation services nationally
- Roll out standardized SDV, cybersecurity, and battery passport frameworks
- Expand AI-driven manufacturing platforms across multiple plants
- Scale national certification stack for future automotive roles
- Integrate MSMEs and startups via shared testbeds

Milestones

- Hundreds of vehicles and subsystems validated annually
- National recognition of CAAR-aligned certifications
- Significant industry uptake of AI manufacturing platforms
- Increased participation in global standards forums

Outcome

CAAR functions as a national platform provider, de-risking innovation and accelerating adoption at ecosystem scale.

Phase 3: Global Leadership (2032–2035)

From National Anchor to Global Reference

Strategic Objective

Position CAAR as a **globally recognized automotive technology authority**, shaping standards, exporting platforms, and influencing global best practices.

Key Initiatives

- Mutual recognition of certifications with global markets
- Leadership roles in international standards bodies
- Export of CAAR-developed platforms and IP
- Hosting global SDV, AI, cybersecurity, and energy forums
- Advanced research into next-generation mobility systems

Milestones

- Global OEMs and suppliers leveraging CAAR validation
- Indian platforms referenced in international standards
- Strong international demand for CAAR-trained professionals
- Sustained IP creation and licensing revenue

Outcome

CAAR evolves into a **global reference institution**, reinforcing India's leadership in secure, software-defined, and sustainable mobility.

11.2 Timeline: CAAR Growth Roadmap

📈 Timeline View (2026-2035)

- **2026-2027:** Labs commissioned, pilots launched, foundations laid
- **2028-2031:** Platforms scaled nationally, certifications mainstreamed
- **2032-2035:** Global recognition, standards leadership, platform exports

Key Insight:

Progression is not linear in outputs—but **exponential in impact**, as platforms and talent compound over time.

11.3 KPI Dashboard: Measuring What Matters

To ensure accountability and continuous improvement, CAAR's impact will be tracked across **three dimensions**: Research, Industry, and Policy & Ecosystem.

KPI Dashboard (Indicative) Research & Innovation Impact

- Patents filed and granted
- Reference architectures released
- Research-to-production conversion rate
- Global citations and collaborations

Industry Impact

- Vehicles and subsystems validated annually
- OEMs, Tier-1s, MSMEs onboarded
- Reduction in recalls and homologation delays
- Adoption of AI manufacturing platforms

Policy & Ecosystem Impact

- Participation and leadership in global standards bodies
- Recognition of certifications domestically and internationally
- Workforce certified per year
- Contribution to sustainability and lifecycle compliance

11.4 Strategic Takeaways

1. **Sequencing matters more than speed**—foundations must precede authority
2. **Platforms compound value** across technology, talent, and compliance
3. **Measurement builds trust** with industry, government, and global partners
4. **Global leadership is earned through consistency, not declaration**

By following this roadmap, CAAR transitions from a respected centre of excellence to a **globally influential automotive technology nerve center**, shaping how the next generation of vehicles are designed, built, secured, and sustained.

Recommended KPI groupings

Research & Innovation

- Patents filed / granted
- Reference architectures released Research → production conversion rate Global collaborations & citations

Industry Impact

- Vehicles & subsystems validated per year OEMs, Tier-1s, MSMEs onboarded Reduction in recalls & homologation delays AI-manufacturing platform adoption

Policy & Ecosystem Impact

- Global standards participation & leadership
- Recognition of CAAR certifications Professionals certified annually
- Lifecycle & sustainability compliance enabled

Section 12
Policy Recommendations

Aligning Government, Industry, and Academia for a Software- Defined Automotive Future

The preceding sections establish that India's automotive competitiveness over the next decade will be determined not by isolated excellence, but by **coordination across institutions, platforms, and talent systems**. The following recommendations are framed to enable **system-level alignment**, while respecting the distinct roles of government, industry, and academia.

Recommendations for Government

Enable Platforms, Not Just Incentives

1. **Recognize and Support Institutional Anchors**
    - Formally recognize institutions like CAAR as **national capability platforms** for SDV, AI, cybersecurity, and lifecycle systems
    - Prioritize long-term institutional funding over short-term project grants
2. **Shift from Compliance-Afterthought to Compliance-by-Design**
    - Encourage early integration of cybersecurity, OTA governance, and AI safety into vehicle development
    - Align domestic requirements with global frameworks (UNECE WP.29, ISO/SAE 21434) to ensure export readiness
3. **Invest in Shared Validation & Assurance Infrastructure**
    - Support shared cyber ranges, AI safety labs, SDV testbeds, and battery lifecycle platforms
    - Reduce duplication of firm-level investments while improving overall ecosystem quality
4. **Strengthen India's Presence in Global Standards Bodies**
    - Enable structured participation of Indian experts and institutions in international standards forums
    - Treat standards engagement as a strategic capability, not an administrative activity

5. **View Talent & Certification as National Infrastructure**
    - Support nationally governed, role-based automotive certifications
    - Align skilling programs with safety-critical, system-level automotive roles

Outcome:

Government shifts from being a regulator and incentive provider to an **enabler of globally competitive automotive systems**.

Recommendations for Industry (OEMs, Suppliers, Startups)

Move from Proprietary Silos to Shared Platforms

6. **Adopt Platform Thinking Over Fragmentation**
    - Collaborate on shared reference architectures, validation frameworks, and testbeds
    - Compete on differentiation, not on recreating foundational infrastructure
7. **Treat Software, AI, and Cybersecurity as Core Capabilities**
    - Retain architectural ownership even when leveraging partners
    - Invest in internal system architects, not just integrators
8. **Embed Security, Safety, and Lifecycle Thinking Early**
    - Integrate cybersecurity, OTA governance, and AI assurance at the design stage
    - Reduce long-term cost and risk associated with recalls and retrofits
9. **Engage Actively with Institutional Platforms**
    - Use neutral institutions for validation, certification, and talent development
    - Support pre-competitive collaboration to accelerate ecosystem maturity
10. **Invest in Workforce Transformation, Not Just Hiring**
    - Align internal role definitions with future automotive system roles
    - Leverage structured certification frameworks to reduce onboarding risk

Outcome:

Industry accelerates innovation while reducing systemic risk, cost, and time-to- market.

Recommendations for Academia & Research Institutions

Translate Knowledge into System Capability

11. **Shift from Research Outputs to System Impact**
    - Prioritize applied research aligned to production, validation, and compliance needs
    - Measure success by adoption and impact, not publications alone
12. **Operate as Ecosystem Integrators, Not Isolated Centers**
    - Collaborate across disciplines—AI, systems engineering, energy, cybersecurity
    - Act as neutral conveners for industry, startups, and regulators
13. **Anchor Talent Development to Real Industry Roles**
    - Design curricula and programs around SDV, AI, cybersecurity, and lifecycle systems
    - Support continuous learning and re-certification models
14. **Participate Actively in Standards & Assurance Frameworks**
    - Contribute technical depth to global standards discussions
    - Help shape future regulations through evidence-based inputs
15. **Build Long-Term Institutional Memory**
    - Preserve and evolve reference architectures, tools, and frameworks across technology cycles
    - Ensure continuity beyond individual projects or funding windows

Outcome:

Academia evolves from a knowledge generator to a **trusted system builder and ecosystem stabilizer**.

Closing Perspective

India's automotive transformation is no longer a question of *whether* the industry will change, but **how coherently it will change**.

The opportunity ahead is not incremental improvement—it is **structural repositioning**:

- From hardware to software-defined platforms
- From compliance to trust-by-design
- From fragmented effort to institutional orchestration

Aligning government policy, industry execution, and academic capability around shared platforms and long-term institutions is the decisive step toward ensuring India's leadership in the next era of global mobility.

Section 13
From Manufacturing Nation to Mobility Technology Leader

India's Opportunity to Define the Next Era of Global Automotive Innovation

For more than three decades, India's automotive success has been built on **manufacturing excellence, scale, and cost competitiveness**. These strengths have enabled India to become one of the world's largest vehicle producers and an integral part of global supply chains.

However, the next phase of automotive evolution will be defined by a different set of capabilities:

- Software-defined architectures
- Artificial intelligence at scale
- Cybersecurity and system resilience
- Energy integration and lifecycle intelligence

In this new paradigm, **value creation is increasingly detached from physical assembly and reattached to technology ownership, trust, and platforms**.

13.1 The Nature of the Transition

The shift from manufacturing leadership to mobility technology leadership is not about abandoning industrial strength—it is about **augmenting it with system-level intelligence and institutional capability**. Manufacturing nations that succeed in this transition will:

- Control software and data architectures
- Shape safety, cybersecurity, and lifecycle standards
- Export platforms, not just products
- Anchor global ecosystems through trusted institutions

Those that do not risk remaining high-volume producers with diminishing strategic leverage.

13.2 Why India Is Uniquely Positioned

India's position in this transition is distinctive.

Unlike legacy automotive powers constrained by decades of entrenched architectures, India combines:

- A rapidly digitizing automotive base
- A globally competitive engineering and software talent pool

- A growing EV and energy ecosystem
- Strong public digital infrastructure
- World-class academic institutions with applied research capability

These factors create a **narrow but powerful window** for leapfrogging—if aligned through shared platforms and long-term institutions.

13.3 Institutions, Not Individual Firms, Will Decide Outcomes

A defining lesson from global automotive leaders is clear:

No nation has achieved sustained automotive leadership through individual firms alone.

Leadership has always been anchored by **institutions that provide continuity, trust, validation, and system integration** across technology cycles.

In the era of software-defined and AI-native mobility, this institutional role becomes even more critical—because complexity, safety, and compliance now exceed the capacity of any single organization.

In addition to academic and standards-oriented institutions, implementation-focused organizations play a critical role in translating cybersecurity, AI safety, and regulatory requirements into operational practice. Institutions such as CyberPeace contribute by addressing vehicle cybersecurity risks across manufacturing and operational environments, supporting safe AI integration, and helping align automotive systems with emerging global regulations such as the EU Cyber Resilience Act—particularly relevant as hybrid and mixed-traffic vehicle environments persist over the next decade.

13.4 The Role of CAAR in the Next Decade

Throughout this whitepaper, CAAR @ IIT Madras has been positioned not as a policy body, regulator, or vendor, but as a **system orchestrator**.

Its role is to:

- De-risk innovation for industry
- Provide neutral validation and assurance
- Build globally aligned platforms and reference architectures
- Develop system-level talent and certification frameworks
- Anchor India's participation in global standards and technology dialogues

In doing so, CAAR can help shift India's automotive narrative—from adoption to authorship.

CAAR as an SDV Ecosystem the Role of Institutional Anchors: Why CAAR Matters

In the context of software-defined and AI-driven mobility systems, the role of an institutional anchor extends beyond research and experimentation. It encompasses ecosystem architecture, standards alignment, and lifecycle validation across multiple technology domains. CAAR is uniquely positioned to serve as such an anchor by providing a neutral environment where OEMs, Tier-1 suppliers, startups, and global technology providers can collaboratively validate SDV architectures, cybersecurity controls, and compliance workflows.

By operating above individual software stacks or platforms, CAAR enables industry participants to focus on innovation while reducing integration friction and regulatory uncertainty. This institutional positioning allows technology providers to demonstrate interoperability, OEMs to de-risk adoption decisions, and policymakers to observe real-world compliance mechanisms. In doing so, CAAR functions not as a competing technology provider, but as a trusted orchestration layer that accelerates the transition from isolated SDV pilots to scalable, market-ready automotive systems.

13.5 A Decade That Will Define India's Mobility Future

The decade from 2026 to 2035 will determine whether India's automotive sector remains primarily a manufacturing powerhouse—or evolves into a **mobility technology leader with global influence**.

The choices made now—about institutions, platforms, talent, and trust—will shape that outcome for decades to come.This whitepaper is not a conclusion, but a **starting point**:

- For coordinated action
- For shared ownership
- For long-term institution building

The opportunity is real. The capability exists. What remains is **alignment and execution**.

Closing Thought

In the next era of mobility, leadership will belong not to those who manufacture the most vehicles—but to those who define how vehicles think, connect, and endure.

Section 14
Global Standards Mapping

Aligning India's Automotive Ecosystem with International Norms

Purpose of This Mapping

As vehicles become **software-defined, AI-driven, cyber-physical, and energy-integrated**, global automotive markets are converging around a **dense web of standards, regulations, and assurance frameworks**.

Compliance is no longer optional.

More importantly, standards participation increasingly determines market access, liability exposure, and long-term competitiveness.

This section maps:

- **Key global standards and regulations**
- Their **functional relevance** across the automotive lifecycle
- **Implications for Indian OEMs, suppliers, startups**
- The **institutional role CAAR can play** in alignment, validation, and participation

1. Global Automotive Standards Landscape (At a Glance)

2. Core Global Standards & Regulations – Mapped by Domain

2.1 Software-Defined Vehicles & OTA

Standard / Regulation	Scope	Why It Matters
UNECE WP.29 (R155 / R156)	Cybersecurity & OTA updates	Mandatory for homologation in many markets
ISO 24089	OTA engineering	Governs safe, auditable software updates
AUTOSAR (Classic & Adaptive)	Vehicle software architecture	De facto global SDV foundation
ASPICE	Software process maturity	Supplier qualification and quality assurance

Implication for India:

SDV readiness is now inseparable from **process maturity and lifecycle governance**.

22 Cybersecurity & AI Safety

Standard / Regulation	Scope	Why It Matters
ISO/SAE 21434	Automotive cybersecurity engineering	Defines threat analysis, risk mitigation
UNECE WP.29 R155	Cybersecurity Management System	Market access requirement
NIST Cybersecurity Framework	Risk-based cyber governance	Increasingly referenced by global OEMs
EU Cyber Resilience Act	Software & OTA liability	Extends responsibility post- sale

Implication for India:

Cybersecurity is no longer a technical function—it is a **regulatory and liability layer**.

23 Functional Safety & AI Reliability

Standard / Regulation	Scope	Why It Matters
ISO 26262	Functional safety	Mandatory for safety- critical systems
ISO 21448 (SOTIF)	Safety of intended functionality	Addresses AI perception edge cases
Emerging AI safety standards (ISO/IEC JTC 1)	AI reliability & explainability	Critical for ADAS & autonomy

Implication for India:

AI-based systems require **probabilistic safety assurance**, not deterministic testing alone.

24 Autonomous Driving & ADAS

Framework	Scope	Why It Matters
SAE J3016	Autonomy level definitions	Global reference language
UNECE ALKS regulations	Level-3 autonomy	Deployment gatekeeper
NCAP protocols	ADAS validation	Consumer trust & ratings

Implication for India:

Most near-term value lies in **resilient ADAS**, not autonomy hype.

25 Electrification, Batteries & Lifecycle

Standard / Regulation	Scope	Why It Matters
EU Battery Regulation	Battery passport & recycling	Mandatory digital traceability
IEC battery standards	Safety & performance	Export compliance
ISO lifecycle assessment (LCA)	Carbon & sustainability	ESG and regulatory reporting

Implication for India:

Battery compliance is shifting from **manufacturing quality → lifecycle transparency**.

2.6 Data, Privacy & Connectivity

Framework	Scope	Why It Matters
GDPR (EU)	Personal data protection	Impacts connected vehicles
Data localization regimes	Sovereignty & compliance	Affects cloud architectures
V2X standards (ETSI / IEEE)	Connectivity & safety	Infrastructure interoperability

Implication for India:

Vehicle data governance is now a **design constraint**, not a legal afterthought.

3. Standards Density vs Capability Gap

Key Observation

Global standards are:

- Increasing in **number**
- Expanding across the **full vehicle lifecycle**
- Shifting liability from **point-of-sale to post-deployment**

However, India's current ecosystem shows:

- Fragmented standards awareness
- Late-stage compliance approaches
- Limited institutional participation in standards drafting

4. Why Institutional Standards Anchors Matter

No major automotive nation relies solely on firms to interpret and comply with standards. Instead, they use **institutions to**:

- Translate standards into engineering practice

- Provide shared validation & test infrastructure
- Represent national interests in global forums
- Reduce compliance cost for industry

5. CAAR's Role in Global Standards Mapping & Alignment

CAAR can act as India's **automotive standards nerve node** by:

5.1 Translation

- Convert global standards into **engineering playbooks**
- Provide reference architectures aligned to standards

5.2 Validation

- Offer pre-certification testing for cybersecurity, OTA, AI safety, batteries
- Reduce homologation delays and rework

5.3 Participation

- Anchor Indian participation in ISO, UNECE, IEC, SAE working groups
- Ensure India is a **co-author, not just an adopter**

5.4 Education

- Embed standards into certification curricula
- Build workforce literacy in regulatory expectations

---

6. Strategic Takeaways

1. **Standards are becoming the real market barriers**
2. **Compliance is continuous, not event-based**
3. **AI and software expand liability horizons**
4. **Institutional mediation reduces cost and risk**
5. **Standards participation equals strategic influence**

Bottom Line

In the next era of mobility, competitiveness will be determined not only by who builds the best vehicles—but by who shapes the standards those vehicles must meet.

This mapping reinforces why **CAAR's role as a neutral, technically credible, standards-anchoring institution is essential** for India's transition from manufacturing scale to mobility technology leadership.

Below is a **concise, executive-ready list** of the **Top 10 Advanced Automotive Companies globally** and **in India**, focused on **technology leadership** (SDV, AI, EVs, autonomy, cybersecurity), along with **company size** (latest publicly available FY23–FY24 scale; rounded for clarity).

I've kept it **board / regulator friendly**—no hype, just signal.

Top 10 Advanced Automotive Companies – Global

Rank	Company	Why They Matter (Tech Leadership)	Size
1	Tesla	SDV-first OEM, OTA-native, AI- driven autonomy, battery tech	$96B revenue
2	Toyota Motor Corporation	Hybrid leadership, software platform Arene, long-term systems thinking	$275B revenue
3	Volkswagen Group	Cariad SDV stack, massive EV scale, OTA push	$350B revenue
4	BYD	Vertical integration (battery + EV), fast innovation cycles	$85B revenue
5	Mercedes-Benz Group	Level-3 autonomy (Drive Pilot), MB.OS	$165B revenue
6	General Motors	Ultifi SDV platform, Cruise autonomy, OTA at scale	$170B revenue
7	Hyundai Motor Group	E-GMP EV platform, robotics (Boston Dynamics), SDV	$185B revenue
8	Bosch	Automotive AI, sensors, cybersecurity, Tier-1 backbone	$95B revenue
9	NVIDIA	De-facto AI compute platform for AVs & SDVs	$61B revenue
10	Stellantis	STLA platforms, software monetization strategy	$200B revenue

Key global pattern:

The leaders either **own the software stack**, **own the battery**, or **own the AI compute layer**.

Top 10 Advanced Automotive Companies – India

(Technology leadership relative to India's ecosystem, not just size)

Rank	Company	Why They Matter (India Context)	Size
1	Tata Motors	EV market leader, software-centric EV platforms	$55B revenue
2	Mahindra & Mahindra	Born-electric platforms (INGLO), OTA focus	$22B revenue
3	Maruti Suzuki	Scale leader, now investing heavily in SDV & EV	$16B revenue
4	Ola Electric	Software-first EVs, in-house OS & battery ambition	$1.5B revenue
5	TVS Motor Company	Connected 2W tech, EVs, digital manufacturing	$4B revenue
6	Ashok Leyland	Electric buses, connected CV platforms	$5B revenue
7	Bosch India	Automotive software, EV components, ADAS	$2B revenue
8	KPIT Technologies	Pure-play SDV, ADAS & mobility software	$1.2B revenue
9	Tata Elxsi	Automotive AI, UX, SDV engineering	$0.5B revenue
10	Ather Energy	Deep software integration in 2W EVs	$0.3B revenue

Key India pattern:

India's strength lies in **engineering talent + EV adoption**, but **system-level IP and standards leadership are still emerging**—which is exactly the gap your whitepaper addresses.

ANNEXURE A
CAAR & the Software-Defined Vehicle (SDV) Ecosystem

(Institutional Architecture & Ecosystem Orchestration View)

Purpose of this Annexure

This annexure provides a **conceptual and visual representation** of CAAR's role within the evolving **Software-Defined Vehicle (SDV) ecosystem**. It is intended to clarify CAAR's positioning as a **neutral institutional anchor** that enables coordination, validation, and governance across multiple technology providers, OEMs, and regulatory stakeholders—without functioning as a commercial technology vendor.

The annexure complements the main policy brief by offering a **system-level perspective** that is especially relevant for:

- Policymakers and regulators
- Global technology partners
- OEM and Tier-1 strategy teams
- Research and standards bodies

Conceptual Framing: CAAR Above the Stack

In the SDV era, value creation increasingly occurs across layered software and hardware ecosystems rather than within isolated components. While individual vendors provide critical SDV building blocks—such as operating systems, middleware, embedded software, digital cockpit frameworks, and AI toolchains—the **integration, validation, and lifecycle governance** of these elements remains a systemic challenge.

CAAR addresses this challenge by operating **above individual SDV stacks**, providing:

- Reference architectures
- Shared validation environments
- Cybersecurity and compliance testbeds
- Neutral coordination across stakeholders

This role ensures that innovation scales safely, securely, and in alignment with global and national standards.

Figure A.1: CAAR & the SDV Ecosystem

Description of the above figure as follows:

CAAR – Institutional Anchor

- Reference Architectures
- Validation & Testbeds
- Cybersecurity & Compliance
- Standards Alignment
- Translational Research

Technology & Solution Ecosystem

(Non-exhaustive, vendor-agnostic)

- Vehicle OS & Middleware
- Embedded & AUTOSAR Platforms
- ADAS / AI & Perception Systems
- Digital Cockpit & UX
- OTA, DevOps & Cloud Toolchains
- Cybersecurity, Identity & Trust Frameworks

These elements represent SDV building blocks provided by global and domestic technology players.

Industry & Market Participants

- OEMs & Vehicle Manufacturers
- Tier-1 & Tier-2 Suppliers
- EV & AV Startups
- Battery & Component Manufacturers
- Fleet Operators & Integrators

Policy & Governance

- Regulators & Ministries
- Standards Bodies (ISO, UNECE, BIS)
- Sustainability & EPR Authorities

Talent & Knowledge Pipeline

- Academic Research
- Workforce Skilling & Certification
- Industry-Academia Collaboration

Key Messages Conveyed by the Visual

1. **CAAR is not a vendor**
   CAAR does not compete with SDV platform providers or system integrators.
2. **CAAR enables coexistence and interoperability**
   Multiple SDV technologies can be validated and integrated within a neutral framework.
3. **CAAR reduces systemic risk**
   By anchoring cybersecurity, lifecycle governance, and compliance early in the design process.
4. **CAAR accelerates market readiness**
   By shortening the path from research and pilots to scalable, compliant deployments.
5. **CAAR strengthens India's global positioning**
   By aligning domestic innovation with international automotive standards and practices.

Policy Relevance

From a policy perspective, this ecosystem model:

- Supports **pre-competitive collaboration**
- Reduces duplication of public R&D investment
- Improves export readiness of Indian automotive products
- Enables regulators to engage with live, validated systems rather than post-hoc audits

Annexure B
References & Sources

A. Global Automotive Strategy & Industry Outlook

1. McKinsey & Company
   The Future of Automotive Software and Electronics McKinsey
   Global Institute, latest editions (2022–2024)

2. Boston Consulting Group (BCG)
   The Software-Defined Vehicle: How OEMs Can Win
   BCG Automotive Practice

3. Deloitte
   2024 Global Automotive Consumer Study
   Deloitte Insights

4. PwC
   Five Trends Transforming the Automotive Industry PwC
   Autofacts

5. World Economic Forum (WEF) The
   Future of Mobility Report
   Centre for the Fourth Industrial Revolution

B. Software-Defined Vehicles (SDV) & Vehicle Architectures

1. AUTOSAR Consortium
   AUTOSAR Classic and Adaptive Platform Specifications
   www.autosar.org

2. SAE International
   SAE J3016 – Taxonomy and Definitions for Levels of Driving Automation

3. ISO
   ISO 24089: Road Vehicles — Software Update Engineering

4. Eclipse Foundation
   SDV Working Group Reports

C. Automotive AI, ADAS & Autonomous Driving

1. ISO
   ISO 21448: Safety of the Intended Functionality (SOTIF)

2. National Highway Traffic Safety Administration (NHTSA), USA
   Automated Driving Systems Safety Principles

3. Euro NCAP
ADAS & Automated Driving Test Protocols

4. NVIDIA
Automotive AI and Autonomous Vehicle Platform Whitepapers

5. Waymo / Cruise / Tesla
Public disclosures, autonomy safety reports, and investor presentations

---

D. Automotive Cybersecurity & AI Safety

1. UNECE
WP.29 Regulations R155 (Cybersecurity) and R156 (Software Updates)

2. ISO / SAE
ISO/SAE 21434: Road Vehicles — Cybersecurity Engineering

3. NIST (USA)
Cybersecurity Framework (CSF)

4. ENISA (European Union Agency for Cybersecurity)
Cybersecurity of Connected and Automated Mobility

5. EU
Cyber Resilience Act (CRA)

E. Electrification, Batteries & Circular Economy

1. European Commission
EU Battery Regulation (EU) 2023/1542

2. International Energy Agency (IEA)
Global EV Outlook

3. IEC
Battery Safety and Performance Standards

4. World Bank
Minerals for Climate Action: The Role of Critical Minerals

5. Ellen MacArthur Foundation
Circular Economy in Mobility

F. Manufacturing, Industry 4.0 & Digital Twins

1. World Economic Forum
Global Lighthouse Network – Advanced Manufacturing

2. Siemens
Digital Twin in Automotive Manufacturing

3. ISO
ISO 9001 / ISO 14001 Quality & Environmental Management

4. Germany Plattform Industrie 4.0
Reference Architectural Model Industrie 4.0 (RAMI 4.0)

G. Workforce, Talent & Skills Transformation

1. World Economic Forum The
Future of Jobs Report

2. OECD
Skills Outlook: Technology and the Future of Work

3. NASSCOM
Automotive & Mobility Skills Report (India)

4. McKinsey Global Institute
Skill Shift: Automation and the Future of the Workforce

H. Standards, Certification & Compliance Governance

1. ISO / IEC
Conformity Assessment & Certification Frameworks

2. TÜV SÜD / TÜV Rheinland
Automotive Certification & Homologation Frameworks

3. International Organization for Standardization
Standards Development and Governance Processes

I. India-Specific Policy & Ecosystem References

1. Government of India
Automotive Mission Plan (AMP) 2016–26

2. NITI Aayog
Advanced Automotive Technology & EV Policy Reports

3. Ministry of Heavy Industries (MHI), India FAME I
& II Policy Documents

4. Bureau of Indian Standards (BIS)
Automotive and EV Standards Notifications

5. IIT Madras
   Research publications, CAAR technical briefs, and institutional material

J. Company Reports & Public Disclosures

1. Annual Reports & Investor Presentations:

Tesla

Toyota Motor Corporation

Volkswagen Group

BYD

Mercedes-Benz Group Tata

Motors

Mahindra & Mahindra

1. Sustainability, Cybersecurity, and Safety Reports published by OEMs and Tier-1 suppliers.

Citation

This whitepaper synthesizes insights from publicly available reports, international standards, regulatory frameworks, academic research, and industry disclosures. Interpretations and recommendations reflect an integrated analysis intended to support strategic decision-making and ecosystem alignment.

ANNEXURE C
Re-Architecting India's Automotive Future

A Policy Brief on Software-Defined, Secure, and Sustainable Mobility

Issued by:

Centre of Excellence in Advanced Automotive Research (CAAR) Indian

Institute of Technology Madras

Executive Summary

The global automotive industry is undergoing its most profound transformation since the advent of mass production. Vehicles are no longer defined primarily by mechanical excellence but by software, data, artificial intelligence, cybersecurity resilience, and sustainability performance. Software-defined vehicles (SDVs), electric mobility, autonomous systems, and digitally governed supply chains are rapidly becoming prerequisites for market access, regulatory compliance, and consumer trust.

For India, this transition presents both a historic opportunity and a strategic risk. While India has emerged as a major manufacturing hub and a fast-growing electric vehicle (EV) market, the supporting digital, cybersecurity, and lifecycle governance infrastructure remains fragmented. Research efforts are often siloed, compliance is addressed late in the development cycle, and startups and MSMEs struggle to navigate regulatory, technical, and ecosystem complexity.

This policy brief argues that India's competitiveness in advanced automotive systems will depend not only on innovation but on **institutional coordination, shared validation infrastructure, and trust-by-design architectures**. It proposes that Centres of Excellence such as CAAR, incubated at IIT Madras, play a pivotal role as neutral, pre-competitive anchors that integrate research, industry, policy, and skills.

The brief outlines global trends, identifies systemic challenges in India's automotive ecosystem, and presents a roadmap for embedding cybersecurity, battery lifecycle governance, and software validation as foundational infrastructure rather than afterthoughts. It concludes with policy recommendations aimed at strengthening India's position in global mobility value chains.

The Global Reset in Automotive Systems

The automotive sector is experiencing a convergence of multiple technology and policy shifts:

- Electrification replacing internal combustion engines
- Software defining vehicle functionality and differentiation
- AI driving perception, control, and optimization

- Cybersecurity becoming a regulatory and safety requirement
- Sustainability and circular economy principles shaping supply chains

Globally, leading OEMs are transitioning from distributed electronic control unit (ECU) architectures to centralized compute platforms supported by virtualization and digital twins. This shift enables over-the-air updates, continuous feature deployment, and lifecycle optimization but also introduces new risks related to software failures, cyberattacks, and systemic vulnerabilities.

Regulators have responded decisively. The UNECE WP.29 framework mandates cybersecurity management systems (R155) and software update governance (R156). The European Union's Battery Regulation introduces battery passports and lifecycle accountability. In the United States, NHTSA has issued cybersecurity best practices, while China has embedded data governance and security into vehicle homologation.

In this environment, automotive competitiveness is increasingly determined by **compliance readiness, validation capability, and digital trust**. Countries that fail to align engineering, policy, and infrastructure risk exclusion from key markets regardless of manufacturing cost advantages.

India's Automotive Opportunity and Structural Challenges

India stands at a critical juncture. The country combines:

- A large domestic automotive market
- Strong engineering and IT talent
- Rapid EV adoption
- A vibrant startup ecosystem
- However, several structural challenges persist.

Fragmentation of Research and Validation

Automotive R&D in India is distributed across OEMs, Tier-1 suppliers, startups, academic labs, and government programs. While this diversity fosters innovation, the absence of shared validation platforms leads to duplication of effort, inconsistent standards interpretation, and high costs—particularly for MSMEs.

Late-Stage Compliance and Export Friction

Cybersecurity, battery compliance, and software safety are often addressed late in product development. This results in redesign cycles, certification delays, and export challenges, especially for companies targeting Europe and other regulated markets.

MSME and Startup Vulnerability

Startups and smaller manufacturers frequently lack access to testbeds, domain experts, and regulatory clarity. As observed in multiple cases, including emerging EV manufacturers, the cost of navigating fragmented institutional interfaces can stall innovation and erode confidence in the ecosystem.

Skills and Talent Mismatch

While India produces large numbers of engineers, industry-ready skills in automotive cybersecurity, SDV architectures, and lifecycle governance remain scarce. Continuous upskilling mechanisms are not yet institutionalized.

Cybersecurity as a Core Automotive Requirement

Cybersecurity has evolved from an IT concern to a **vehicle safety and national security issue**. Modern vehicles integrate connectivity, cloud services, AI models, and third-party software components, dramatically expanding the attack surface.

Regulatory frameworks such as UNECE R155 require OEMs to demonstrate risk management across the vehicle lifecycle, including supply chain security, incident response, and continuous monitoring. Compliance is not a one-time certification but an ongoing process.

In India, while awareness of automotive cybersecurity is increasing, structured validation environments remain limited. There is a need for neutral testbeds that allow manufacturers to assess vulnerabilities, validate controls, and align with international standards without exposing proprietary information.

Institutions like CAAR are uniquely positioned to host such environments, combining academic rigor with industry relevance and policy alignment.

Battery Lifecycle Governance and Circular Economy

EV batteries represent both a strategic asset and a governance challenge. Issues include:

- Traceability of materials and components
- Compliance with safety and recycling regulations
- Carbon footprint accounting
- Second-life utilization and material recovery

The EU Battery Passport initiative exemplifies how digital identity, lifecycle data, and compliance credentials are becoming mandatory for market access. India's Battery Waste Management Rules and Extended Producer Responsibility (EPR) frameworks signal a similar trajectory.

Without digital lifecycle infrastructure, manufacturers face compliance risk, recyclers struggle with traceability, and policymakers lack real-time visibility. Blockchain-enabled lifecycle passports, supported by IoT and AI analytics, offer a viable solution—but only if implemented within trusted, neutral governance structures.

From Pilots to Platforms: Rethinking Public R&D Investment

A recurring challenge in India's innovation ecosystem is the proliferation of isolated pilots. While pilots demonstrate feasibility, they often fail to scale or interoperate.

This brief advocate a shift toward **platform-centric investment**, where shared infrastructure—testbeds, reference architectures, data models, and certification pathways—supports multiple innovations over time.

Such platforms lower entry barriers for MSMEs, reduce duplication, and ensure policy continuity. CAAR-hosted platforms for cybersecurity validation and battery lifecycle governance exemplify this approach.

Workforce Development as Strategic Infrastructure

Advanced automotive systems demand interdisciplinary skills spanning mechanical engineering, software, AI, cybersecurity, and regulatory compliance. Traditional curricula alone are insufficient.

Policy should recognize workforce development as infrastructure, supporting:

- Modular certification programs
- Industry-academia co-designed curricula
- Continuous learning linked to evolving standards

Centres of Excellence can serve as hubs for such initiatives, aligning training with real-world validation environments.

Policy Recommendations

Based on the analysis, this brief proposes the following actions:

1. **Support Institutional Anchors:** Strengthen Centres of Excellence as neutral platforms for validation and compliance.
2. **Embed Cybersecurity Early:** Encourage design-stage integration of cybersecurity through incentives and guidelines.
3. **Implement Battery Lifecycle Infrastructure:** Develop national frameworks for battery passports aligned with global standards.
4. **Reduce Ecosystem Fragmentation:** Promote shared testbeds and reference architectures.

5. **Enable MSME Participation:** Subsidize access to validation infrastructure and expertise.
6. **Align Skills with Standards:** Integrate training with regulatory and technical frameworks.

Roadmap 2025–2035

Phase 1 (2025–2027): Foundation

- Establish shared testbeds
- Pilot battery lifecycle systems
- Develop certification frameworks

Phase 2 (2027–2031): Scale

- Expand industry participation
- Integrate with export compliance systems
- Build talent pipelines

Phase 3 (2031–2035): Leadership

- Position India as a global reference for secure, sustainable mobility
- Influence international standards
- Enable cross-border interoperability

Conclusion

India's automotive future will be defined not only by manufacturing capacity but by its ability to deliver **secure, software-defined, and sustainable mobility systems**. This requires moving beyond fragmented innovation toward coordinated platforms anchored by trusted institutions.

CAAR's evolving role illustrates how academic excellence, industry collaboration, and policy foresight can converge to address systemic challenges. By investing in institutional capacity and shared infrastructure, India can transform compliance from a constraint into a competitive advantage and emerge as a leader in advanced automotive systems.

Annexure D
CAAR: Emerging as the Nerve Center of Advanced Automotive Industry

CAAR & the Software-Defined Vehicle (SDV) Ecosystem

A Neutral, Research-Led Platform for the Future of Advanced Automotive Systems

CAAR – Centre of Excellence in Advanced Automotive Research
Incubated at IIT Madras

About CAAR

CAAR (Centre of Excellence in Advanced Automotive Research), incubated at IIT Madras, is a research-driven, industry-connected institution dedicated to advancing next-generation automotive technologies. CAAR operates at the intersection of mobility engineering, cybersecurity, AI, electronics, and policy, enabling translational research that moves seamlessly from lab to real-world deployment.

Why Software-Defined Vehicles Need a New Kind of Ecosystem

The global automotive industry is rapidly transitioning toward Software-Defined Vehicles (SDVs), where software, data, AI, and connectivity define vehicle functionality, safety, and lifecycle value.

This shift introduces:

- Exponential growth in software complexity
- Expanded cyber-attack surfaces
- New regulatory obligations (UNE WP.29, ISO/SAE 21434)
- The need for continuous validation, OTA assurance, and digital traceability
- Tight coupling between hardware, software, cloud, and edge systems

CAAR as an Institutional Anchor

Reference Architectures	Validation & Testbeds	Cybersecurity & Compliance	Standards Alignment

Ecosystem Participants

- OEMs & EV Manufacturers
- Tier-1 & Tier-2 Suppliers
- Automotive software & SDV platform companies
- Semiconductor and embedded/IP solution providers
- AI, cybersecurity & cloud technology firms
- Startups building deep-tech automotive solutions
- Government and standards bodies
- Academic and research institutions

CAAR's Role in the SDV Value Chain (Focus Areas)

01
Architecture & Systems Thinking
Reference architectures for SDV platforms, secure E/E architectures, gateways, and centralized compute

02
Cybersecurity & Trust
Vehicle, battery, and component identity & traceability; secure OTA, PKI, and cryptographic lifecycle management

03
AI-Driven Engineering
AI for manufacturing automation and quality analytics; AI-assisted anomaly detection, cloud analytics, and regulatory dashboards

04
Validation & Testbeds
Neutral labs and testbeds for SDV, ADAS, EV, and connected systems, including Hardware-in-the-Loop (HIL), Software-in-the-Loop (SIL), cloud simulation, and industry pilots with OEMs and Tier-1s

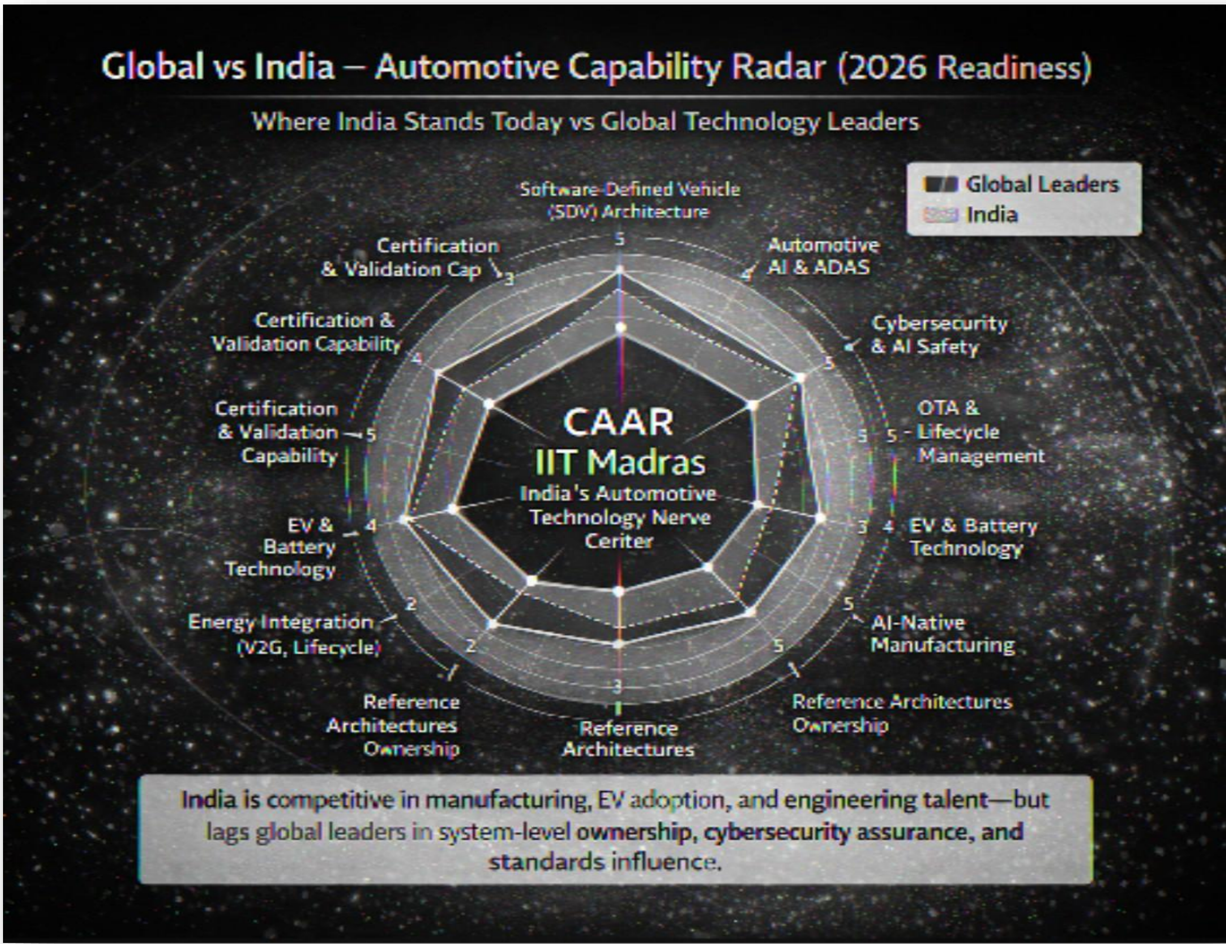
05
Policy, Standards & Workforce
SDV policy development, standards alignment, and workforce readiness at national and global levels

The CAAR Opportunity

As the automotive industry evolves toward SDVs, CAAR offers partners:

Faster innovation cycles	Reduced integration and compliance risk	Shared infrastructure and neutral validation platforms	Access to a growing ecosystem of industry and research collaborators

For collaboration, pilots, and research partnerships, engage with CAAR at IIT Madras.


Global vs India – Automotive Capability Radar (2026 Readiness)
Where India Stands Today vs Global Technology Leaders
Global Leaders
India
Software-Defined Vehicle (SDV) Architecture
Automotive AI & ADAS
Cybersecurity & AI Safety
OTA & Lifecycle Management
EV & Battery Technology
AI-Native Manufacturing
Reference Architectures Ownership
Reference Architectures
Reference Architectures Ownership
Energy Integration (V2G, Lifecycle)
EV & Battery Technology
Certification & Validation Capability
Certification & Validation Capability
Certification & Validation Cap
CAAR
IIT Madras
India's Automotive Technology Nerve Center
India is competitive in manufacturing, EV adoption, and engineering talent—but lags global leaders in system-level ownership, cybersecurity assurance, and standards influence.