RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

TELECOM Paris

INSTITUT POLYTECHNIQUE DE PARIS

FONDATION Mines-Télécom
La Fondation de l'IMT

ICMS CHAIR

FIRST WHITE PAPER

January 2026

INTRODUCTION

The evolution of the automotive industry has reached an inflection point. Beyond the widespread adoption of electrification, vehicles are becoming increasingly connected, paving the way for more user-centric services and autonomous mobility.
These objectives drive the embedded E/E architecture towards a more centralized SDV (Software Design Vehicle) architecture, merging features for better performance, scalability, updatability, and cost optimization. In parallel, new technologies like AI and Quantum Computing are maturing and becoming applicable in the cyber domain, presenting both opportunities... and new threats.

Today, we could consider that the vehicle protection relies on three pillars and challenges:

1. **Cybersecurity by design**, which is the foundation based on a defense-in-depth strategy.

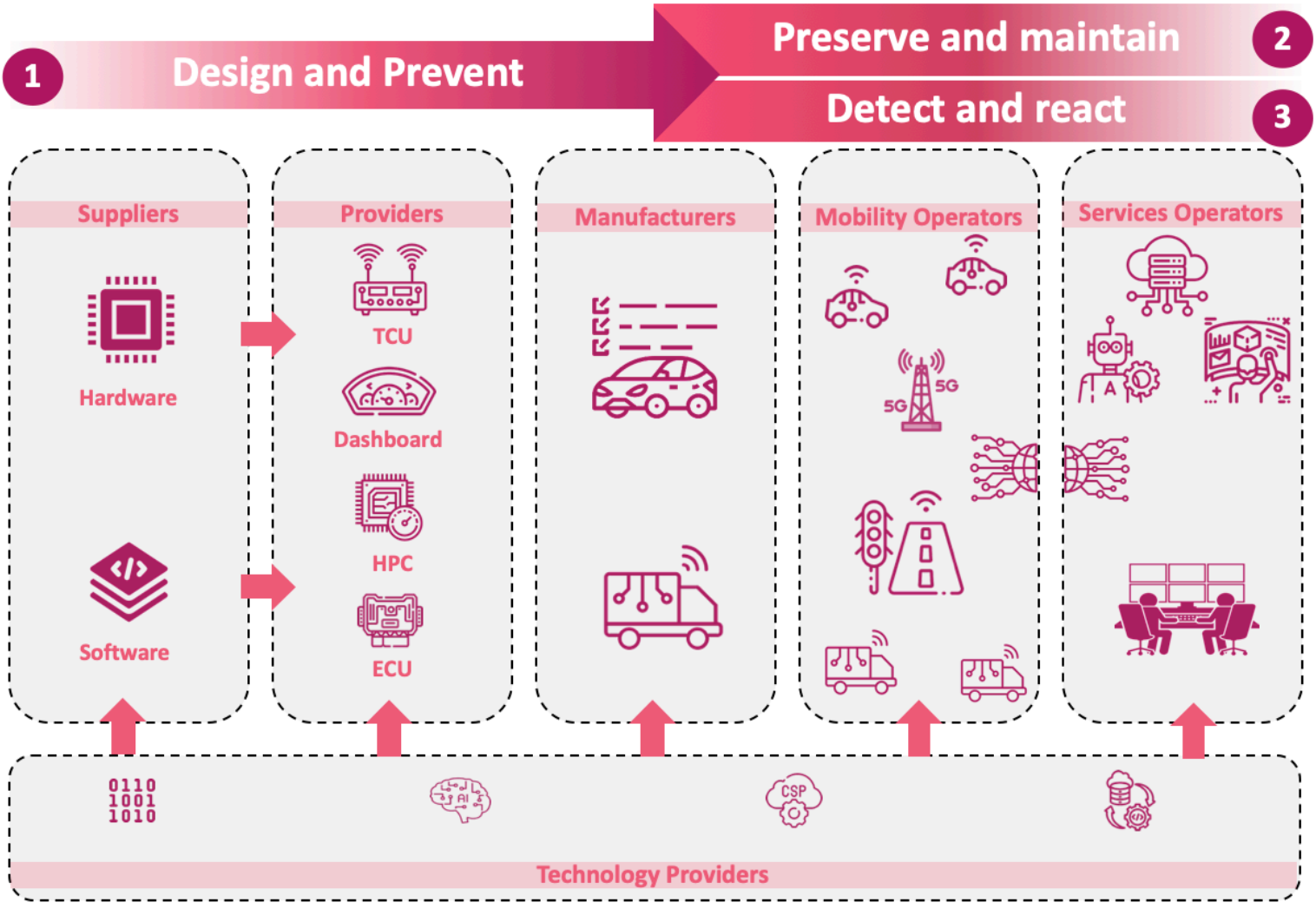
2. **Detection and reaction**, which complements the first pillar. If an attacker breaches the protections, the objective is to detect the attack and react within a timeframe compatible with the threat level.

3. **Preserve and maintain**, ensuring that the vehicle remains cyber secure throughout its lifecycle, which could exceed 15 years—a real challenge!

Indeed, while these advancements unlock groundbreaking functionalities —such as enhanced interconnectivity, communication with external systems, and embedded power—they also introduce unprecedented cybersecurity challenges. The proliferation of embedded electronics and software in vehicles has significantly expanded the attack surfaces, making the protection of their integrity, reliability, and the privacy of occupants more challenging than ever.
Additionally, the threat landscape has evolved and continues to do so. The skills of attackers are improving, not least through ever more powerful AI, which means that integrated cyber security measures need to be constantly reinforced.
Last but not least, the number of cybersecurity regulations is also increasing, with European texts such as GDPR for privacy, UNR155 based on ISO21434, and Euro7/Antitampering for automotive, as well as the CRA (Cyber Resilience Act) for all industries. Other regulations, decrees, and jurisprudence in countries like China, the US, and Russia also contribute to a new situation for the security of mobility system.

Recognizing the urgency of addressing these challenges, the Intelligent Cybersecurity for Mobility Systems (ICMS) chair was launched in February 2024 by Telecom Paris.
Supported by seven key world-leading industrial partners (BCG, Ampere & Renault Group, Solent, Thales, Valeo, ZF) and the SystemX Applied Research Institute, ICMS aims to create a robust platform for research and innovation in connected vehicle cybersecurity. Building on the foundation of the earlier C3S chair, ICMS seeks to push the boundaries of knowledge in this field, aligning cutting-edge academic research with the immediate and long-term needs of the automotive and mobility industries.

The purpose of this white paper is to introduce the vision, objectives, and scientific and technical challenges that underpin the ICMS initiative. With a collaborative framework involving prominent industry and academic leaders, ICMS strives to deliver innovative and actionable solutions throughout the automotive value chain. Its focus spans critical areas such as risk analysis and assessment, development of cryptographic architectures, by design data protection and intrusion detection and cyber-resilience, all while addressing the unique demands of connected and autonomous vehicles.



AMBITION

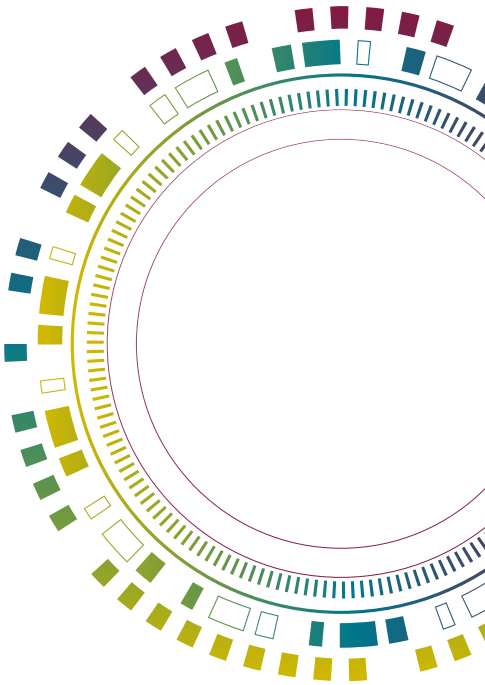
The ICMS research chair is dedicated to addressing the evolving cybersecurity challenges in modern and future mobility ecosystems.

We focus on integrating cybersecurity throughout the entire vehicle lifecycle, from risk assessment and secure design to real-time intrusion detection and cryptographic agility. By leveraging advancements in AI, ML and cryptography, the chair develops cutting-edge security frameworks that protect vehicle networks, ensure data privacy and improve system resilience against emerging threats.

We have created a research chair to develop international collaboration and meet the challenges of cybersecurity in mobility systems. By linking industry, universities and laboratories, we are fostering innovation and accelerating the deployment of cybersecurity solutions in the real world. Our aim is to become a global reference by addressing the following key objectives, from design to operational:

- Developing AI-powered cybersecurity frameworks for connected and autonomous vehicles.
- Enhancing intrusion detection and response mechanisms using federated learning and embedded AI.
- Ensuring secure communication and data privacy across vehicular networks.
- Mitigating emerging threats, such as adversarial AI, sensor spoofing, and supply chain vulnerabilities.

Positioned as an **international research chair**, ICMS will establish best practices, influence regulatory frameworks, and accelerate the deployment of advanced cybersecurity solutions in mobility ecosystems. By harnessing breakthroughs in AI/ML, cryptography, and secure system design, the ICMS chair aims to set new standards for cybersecurity in mobility systems, ensuring safety, trust, and resilience across the mobility sector.



CHALLENGES

The ICMS Chair explores a new frontier in mobility cybersecurity, driven by increasing vehicle connectivity, autonomy and software integration, all of which extend the attack surface.

A first scientific challenge is to develop robust risk analysis methodologies that combine cybersecurity and functional safety, while considering the evolution of threats throughout the vehicle lifecycle.
Real-time detection of intrusions and misbehaviour is another major focus: as vehicles become software-defined and AI-driven, lightweight onboard systems are needed to detect and respond to AI-driven stealth attacks with a minimum of false positives.

Data protection and privacy are also essential. Connected vehicles process large quantities of sensitive data, which requires technical and regulatory safeguards. ICMS is investigating privacy-enhancing technologies such as federated learning and secure multi-party computing to ensure compliance with GDPR, NIS2 and related frameworks while supporting innovation. The regulatory landscape itself presents a challenge, as the industry must now navigate the overlapping and sometimes conflicting requirements of GDPR, the Cyber Resilience Act, UN R155, ISO21434, ... Finding a balance between data sharing and the protection of privacy and security is a complex but essential objective.

Other research priorities include the design of agile and future-proof cryptographic architectures, especially in anticipation of quantum threats, as well as secure vehicle and user identity management.

Finally, ICMS promotes resilience by design, integrating proactive and dynamic defense mechanisms such as Moving Target Defense and system reconfiguration early in development. Together, these challenges define a multidisciplinary research program at the intersection of embedded systems, cybersecurity, AI, cryptography and automotive engineering.

CONSORTIUM

The ICMS research chair is a dynamic collaboration between leading industrial and academic partners, uniting expertise from the automotive, cybersecurity, consulting, and research sectors to address the most pressing cybersecurity challenges in mobility systems. Each partner brings unique strengths to develop cutting-edge solutions and drive innovation in secure and safe mobility.

Renault Group & Ampere – As leading automotive manufacturers, they provide deep knowledge in vehicle architectures, embedded systems, and secure software updates. Their role focuses on integrating cybersecurity into vehicle design and ensuring security compliance across their fleets.

ZF – A global technology company specializing in automotive systems, ZF brings expertise in vehicle motion control, safety systems, and secure over-the-air updates, ensuring robust cybersecurity measures for intelligent mobility solutions.

Valeo – A leader in automotive innovation, Valeo focuses on securing ADAS (Advanced Driver-Assistance Systems) and electrification technologies, ensuring resilience against cyber threats in connected and autonomous vehicles.

Thales – A global leader in cybersecurity and secure communications, Thales brings expertise in encryption, intrusion detection, and AI-powered threat mitigation, with a particular focus on securing vehicular networks and critical automotive infrastructure.

Solent – A key player in cyber resilience, Solent contributes to intrusion and misbehavior detection by developing advanced machine learning models for real-time anomaly detection and response within mobility systems.

BCG – As a strategic consulting firm, BCG provides insights into worldwide automotive market trends and perspectives, cybersecurity governance, risk management frameworks, and regulatory compliance, helping to bridge the gap between technical advancements and industry-wide adoption.

SystemX – A leading Institute for Technological Research (IRT) specializing in digital transformation, SystemX contributes research expertise in secure system design, cybersecurity risk assessment, and the development of technology platforms for automotive security validation.

ICMS EMBEDDED SECURITY FRAMEWORK: A PRACTICAL SOLUTION

To support the work of researchers, industry professionals, and all contributors to the mobility cybersecurity ecosystem—including public authorities, regulators, technology providers, and data suppliers—ICMS aims to develop a practical framework for analyzing and classifying the key dimensions and levers that contribute to the security of embedded systems.

This framework will serve as a robust foundation for positioning challenges and solutions addressed in the research programs led by the chair, but also by state-of-the-art references. It will enable the comprehensive mapping of cybersecurity challenges and innovative solutions onto a two-dimensional grid, making them easier to interpret, visualizing their interactions, and defining their scope. Beyond positioning, this analytical grid could also serve as a normative basis for assessing both existing cybersecurity maturity levels (evaluation) and target maturity levels (goals) for systems, projects, or organizations dealing with cybersecurity and mobility.

This approach—combining key cybersecurity dimensions with the product lifecycle—aims to:

- Provide a comprehensive view of risks and necessary actions.
- Enable an objective measurement of system maturity.
- Foster collaboration between industry, researchers, and regulators to enhance ecosystem security.

More precisely, similar to the NIST Cybersecurity Framework (CSF), which organizes cybersecurity capabilities in a quasi-chronological approach (Governance, Identification, Protection, Detection, Response, and Recovery), our two-dimensional grid will permit us to develop an analytical methodology to integrate these cybersecurity dimensions with the key stages of the product and service lifecycle in mobility (HW/SW design, quality assurance, assembly, deployment, maintenance, and monitoring).

This shared and coherent approach will act as a reference framework for product integration and for measuring the resulting cybersecurity maturity at the scale of a product line, an organization, or even an entire ecosystem.

This framework will be meticulously developed and rigorously tested in collaboration with researchers and industry professionals throughout the life cycle of the chair, ensuring its relevance and applicability in real-world scenarios.

CHAIR AXES

The ICMS Chair technical axes outlines several key research topics aimed at enhancing the security, functionality, and privacy of embedded systems, particularly in the automotive context. In more details, we have defined the six following axes.

1. Risk Analysis:

This axis emphasizes integrating operational safety and cybersecurity risk management during the design of automotive embedded systems. It addresses challenges such as evolving threats, regulatory changes, AI integration, and rapid technological advances. The goal is to develop lifecycle-spanning design methods that adapt to diverse and evolving risks.

2. Intrusion and Misbehaviour Detection:

Focused on dynamically detecting attacks during a vehicle's lifetime, this axis uses AI and machine learning to identify anomalies in vehicle behaviour. Challenges include characterizing normal behaviour, handling novel attack types, minimizing false positives, and enabling real-time processing within the vehicle.

3. Digital Regulations' Impacts on Connected Vehicles:

This axis examines regulatory and technical solutions for safeguarding the confidentiality of personal and non-personal data in intelligent mobility systems. It explores the sensitivity of data, privacy-enhancing technologies (PET), cybersecurity governance and control, regulatory inconsistencies, and promoting data sharing while respecting privacy rights and data security. It studies the impacts of the growing complexity of digital regulations in the automotive industry.

4. Cryptographic Architecture and Agility:

With vehicles serving as data hubs, this axis proposes secure, long-term cryptographic solutions to protect sensitive data. It includes designing efficient V2X protocols, addressing quantum threats, and ensuring agile updates to security mechanisms to handle emerging threats.

5. Authentication, Identity, and Behavioural Signatures:

This axis targets secure digital identity systems for modern vehicles, covering access control, secure communications, and software updates. It highlights key management systems, secure battery charging communications, and a trusted security controller for ECU and infotainment networks.

6. Resilience by Design:

To counter attackers' ability to learn defence strategies, this axis investigates incorporating proactive defence mechanisms like «Moving Target Defence» during system design. It aims to enhance system resilience by dynamically **reconfiguring components, balancing security with service continuity, and validating deployment strategies.**

CONCLUSION

The ICMS chair represents a pivotal step toward advancing cybersecurity in mobility systems, fostering innovation at the intersection of industry and academia. But we can't succeed on our own, and we believe it's essential to strengthen our existing consortium. Hence, to maximize its impact, we invite additional industrial partners to join this initiative, contribute their expertise, and shape the future of secure mobility. We also open the dialogue and a collaboration with other chairs to create a robust, shared knowledge European ecosystem in cybersecurity. Finally, we seek to build strong ties with international academic institutions to foster cross-border research and elevate global standards in automotive cybersecurity.

ACKNOWLEDGMENT

This work is conducted within the Intelligent Cybersecurity for Mobility Systems (ICMS) research chair at Télécom Paris, founded by Ampere, BCG, IRT SystemX, Renault, Solent, Thales, Valeo, and ZF Group, and supported by the Fondation Mines-Télécom.