AUTOCRYPT

AUTOCRYPT E2E CYBERSECURITY FOR ADS SAFETY

AUTOCRYPT'S CYBERSECURITY STRATEGY FOR AUTONOMOUS DRIVING

"AUTOCRYPT's End-to-End (E2E) Cybersecurity framework presents an integrated security approach spanning the entire autonomous driving ecosystem — including OEMs, autonomous driving developers, mobility platform providers, and insurers — designed to ensure the safety, reliability, and trustworthiness of autonomous driving systems."

TABLE OF CONTENTS

INTRODUCTION: CYBERSECURITY FOR AUTONOMOUS DRIVING

Autonomous Driving Systems (ADS) combine artificial intelligence (AI), sensor fusion, high-performance computing, and connectivity technologies to enable vehicles to perceive, decide, and operate without direct human intervention. Using cameras, radar, LiDAR, and other sensing technologies, autonomous vehicles continuously interpret surrounding environments and execute driving decisions in real time. As autonomous driving advances, it is increasingly recognized as a key driver transforming the automotive industry into an intelligent mobility service ecosystem.

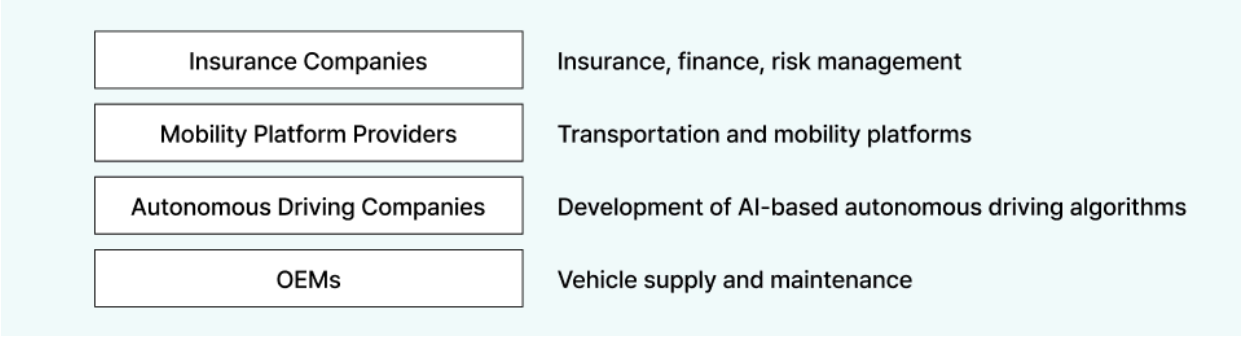
The evolution of autonomous driving is accelerating the transition toward electrification and Software-Defined Vehicles (SDVs), increasing connectivity between in-vehicle systems and external infrastructure. As vehicles evolve into Cyber-Physical Systems (CPS), expanded connectivity becomes essential for autonomous driving capabilities while also significantly enlarging the cyberattack surface across the vehicle ecosystem.

Within this context, cybersecurity has become a foundational requirement for ensuring the safety and reliability of autonomous driving systems. Unlike conventional automotive cybersecurity threats, attacks targeting autonomous vehicles can directly impact physical safety through remote vehicle manipulation, sensor spoofing, and exploitation of software vulnerabilities. This risk becomes even more critical in autonomous driving systems incorporating Physical AI elements, where cyberattacks can directly influence real-world vehicle behavior and potentially lead to physical safety incidents.

For autonomous driving technologies to achieve successful commercialization and public acceptance, cybersecurity must be regarded as a core safety foundation rather than an optional feature. Failure to adequately address cybersecurity risks could result not only in isolated incidents, but also in broader erosion of trust across the autonomous mobility industry. Therefore, cybersecurity must be embedded as a fundamental design principle throughout the autonomous driving ecosystem, supported by both technological safeguards and institutional governance frameworks.

AUTONOMOUS DRIVING ECOSYSTEM

The autonomous driving industry is a complex ecosystem composed of vehicles, software, services, and regulatory frameworks, making collaboration among multiple stakeholders essential. For example, integrated ecosystems involving OEMs, autonomous driving companies, mobility service providers, and insurers are becoming increasingly important. One example is South Korea's "K-Autonomous Driving Collaboration Model," which establishes a unified framework coordinating vehicle supply, insurance, and mobility service operations across the autonomous driving ecosystem to support aligned ecosystem development.



Autonomous driving companies play a central role in developing AI-based autonomous driving algorithms and continuously improving system performance using real-world driving data. Yet, autonomous driving technologies are closely interconnected with vehicle control, safety assurance, and service operations, companies face structural limitations in independent development and large-scale validation.

To address these challenges, **OEMs** provide vehicles optimized for autonomous driving validation and standardized vehicle control interfaces. In addition, they establish real-time data pipelines that deliver vehicle-generated data while also supporting vehicle condition monitoring and maintenance, creating an environment that enables autonomous driving companies to focus on core software development.

Mobility platform providers are responsible for autonomous driving service operations and data utilization. They provide the platforms required for fleet management, dispatch operations, and driving data analytics while validating operational efficiency and service stability in real-world deployment environments through integration between vehicles and mobility platforms.

In autonomous driving environments, accidents may occur due to unpredictable road conditions, systems failures, or cyberattacks. **Insurers** help mitigate this risk by providing accident data analysis, accident prevention consulting, and other risk management services that contribute to improving the safety and reliability of autonomous driving systems. This also helps reduce liability risks, one of the major barriers to the commercialization of autonomous driving technologies.

AUTONOMOUS DRIVING CYBERSECURITY: SINGLE-LAYER SECURITY

Autonomous driving systems are composed of multiple interconnected layers, including in-vehicle control systems, autonomous driving software, cloud and mobility platforms, and data infrastructure. Due to this multi-layered architecture, Single-Layer Security — the practice of protecting only a single layer — is insufficient to fundamentally ensure the safety and reliability of autonomous driving systems. In some cases, security approaches focused on a single layer may even obscure broader system vulnerabilities or concentrate risks within specific points of failure.

Single-Layer Security approaches fundamentally fail because attackers tend to target the exploit the most vulnerable layer within interconnected systems. Rather than directly attacking heavily protected in-vehicle systems, attackers are more likely to exploit indirect attack paths such as external platforms, cloud APIs, or mobile applications. As a result, vulnerabilities within a single layer can still enable attacks that compromise the broader autonomous driving ecosystem.

Moreover, interfaces between layers also serve as critical attack surfaces within autonomous driving environments. Data continuously moves across vehicles, cloud systems, mobility platforms, and external services, and if authentication, encryption, and integrity validation are not consistently applied throughout this process, attackers may manipulate data or hijack sessions to disrupt system operations. While Single-Layer Security may be effective in protecting individual domains internally, its inability to secure boundary areas where data is exchanged limits its ability to defend against realistic attack scenarios.

Even from a governance perspective, Single-Layer Security carries structural limitations in environments involving multiple stakeholders and distributed operational responsibilities. Autonomous driving ecosystems consist of various stakeholders — including OEMs, autonomous driving companies, mobility platform providers, and insurers — each operating different systems and security policies. In such distributed environments, insufficient security within a single layer can create security gaps that affect the entire system. Thus, appropriate cybersecurity measures must be consistently applied across all layers of the autonomous driving ecosystem.

AUTONOMOUS DRIVING CYBERSECURITY: LAYER-BY-LAYER SECURITY

Autonomous driving systems are multi-layered distributed systems composed of various interconnected domains, where each later operates as part of a unified service environment. A commonly adopted cybersecurity approach within this type of structure is Layer-by-Layer Security — applying independent security measures to each individual layer. However, for complex cyber-physical systems such as autonomous driving, this approach alone is insufficient to ensure comprehensive safety and security. Applying security technologies to each separate layer may be a necessary condition for autonomous driving cybersecurity, but not a sufficient one.

The most critical limitation of the Layer-by-Layer Security approach is inconsistency in security policies. As each layer is operated by different organizations, authentication methods, encryption standards, and access control policies may vary significantly across the ecosystem. In such environments, attackers intentionally target the layer with the weakest security posture to bypass the broader system.

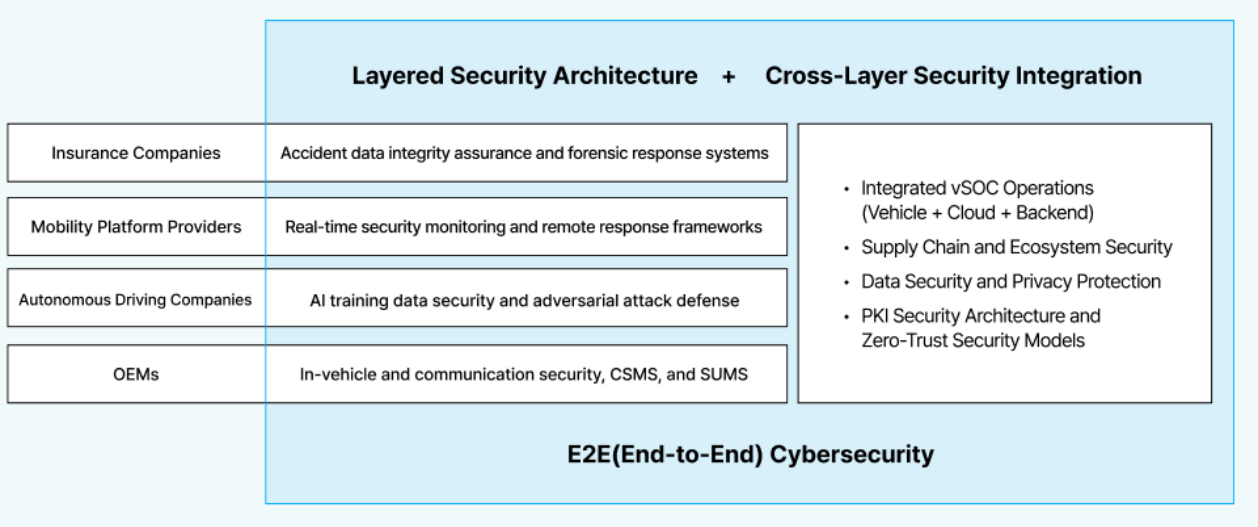
This means that even if strong authentication mechanisms are implemented within in-vehicle systems, relatively weaker authentication methods used in mobile applications or mobility platforms can become attack points that indirectly provide access to the entire ecosystem. In other words, even if individual layers are independently secure, inconsistencies between security policies themselves can become new attack surfaces.

In addition, attacks within autonomous driving environments no longer occur at a single point, but instead evolve into chained attacks that combine vulnerabilities across multiple layers. Even if vulnerabilities identified within individual layers are not critical on their own, linking them together can create attack paths capable of compromising the entire system. For instance, attackers may exploit vulnerabilities within a mobile application to steal authentication tokens, use those credentials to access cloud APIs, and ultimately deliver malicious vehicle control commands. These interconnected attacks are difficult to detect and block through isolated layer-specific security approaches alone.

Lack of security visibility across the overall architecture also presents a critical challenge, as activities that appear normal within individual systems may actually form part of a coordinated attack scenario. For example, even if mobile application logins, cloud API requests, and vehicle control commands appear legitimate when viewed separately, they may reveal abnormal attack patterns when analyzed collectively. As a result, Layer-by-Layer Security architectures often struggle to identify the broader attack context, increasing the likelihood of delayed detection and failed response efforts.

AUTOCRYPT E2E CYBERSECURITY FRAMEWORK

AUTOCRYPT's End-to-End (E2E) Cybersecurity framework for autonomous driving defines cybersecurity not as a single technology, but as a structured architecture spanning all layers of the ecosystem to ensure system safety and reliability. This model is built upon two core pillars — Layered Security Architecture and Cross-Layer Security Integration — and follows the principle of "Security for Safety," recognizing that cybersecurity incidents can directly lead to physical safety risks.



The first pillar of this framework, Layered Security Architecture, applies independent yet specialized cybersecurity technologies across each layer of the autonomous driving ecosystem. Leveraging AUTOCRYPT's full-stack automotive cybersecurity portfolio and specialized security expertise, optimized layer-specific security technologies are implemented based on threat analysis processes tailored to the unique characteristics of each domain.

Going one step further, AUTOCRYPT emphasizes that meaningful safety cannot be guaranteed unless layer-specific security systems are organically interconnected. This is where the second pillar, Cross-Layer Security Integration, becomes essential. Rather than operating independently, this approach integrates the security systems of each layer into a unified operational framework capable of detecting, responding to, and preventing attacks from an end-to-end perspective.

AUTOCRYPT's E2E Cybersecurity is not simply a collection of multiple security technologies, but an optimized cybersecurity framework that combines multi-layered defense structures with cross-layer integration. While Layered Security Architecture provides specialized protection for each layer, Cross-Layer Security Integration connects these layers to establish system-wide consistency and visibility. Only when these two elements operate together can autonomous driving systems effectively respond to complex attack scenarios and chained threats, ultimately realizing the goal of "Safety through Security."

LAYERED SECURITY ARCHITECTURE + CROSS-LAYER SECURITY INTEGRATION

Within the AutoCrypt E2E Cybersecurity framework, Layered Security Architecture defines threat models for each layer of the autonomous driving system and applies security technologies optimized for the specific characteristics of each domain.

- **OEMs** implement encryption and authentication systems to prevent leakage and tampering of critical in-vehicle software while securing both internal and external vehicle communications, In addition, they establish Cyber Security Management Systems (CSMS) and Software Update Management Systems (SUMS) to manage cybersecurity throughout the vehicle lifecycle.
- **Autonomous driving companies** ensure the integrity of AI training data, manage software vulnerabilities, and implement AI safety guardrails capable of monitoring incorrect AI decisions caused by adversarial attacks.
- **Mobility platform providers** perform real-time security monitoring, data encryption, and privacy protection across the service layer connecting vehicles and cloud infrastructure.
- **Insurers** establish accountability and trust through accident data tamper prevention mechanisms and forensic-based validation systems.

In this way, each stakeholder maintains security architectures around its own threat model, collectively forming the foundational defense layer of the autonomous driving ecosystem.

As autonomous driving systems operate as tightly interconnected ecosystems rather than isolated environments, attacks also occur across layer boundaries. This is where Cross-Layer Security Integration becomes essential. Rather than deploying security functions independently across each layer, this approach consistently integrates policies, authentication, data management, and monitoring throughout the entire ecosystem.

A representative example is the integrated Vehicle Security Operations Center (vSOC), which collectively analyzes logs and events generated from vehicles, cloud systems, and mobility platforms to identify attack patterns that may be difficult to detect within isolated layers. In addition, PKI-based integrated authentication frameworks enable mutual verification among all communication entities, while Zero Trust architectures eliminate the assumption that internal systems are inherently trustworthy.

Furthermore, supply chain security also serves as a critical component within this framework. Autonomous driving systems are composed of numerous suppliers and software components, making it possible for vulnerabilities originating from hardware and software supply chains to propagate throughout the broader ecosystem. As a result, end-to-end supply chain security management spanning the entire lifecycle — from development and deployment to operations — becomes essential.

About AUTOCRYPT

AUTOCRYPT is a leading player in automotive cybersecurity and smart mobility technologies. It specializes in the development and integration of security software and solutions for in-vehicle systems, V2X communications, Plug&Charge, and fleet management, paving the way toward a secure and reliable C-ITS ecosystem in the age of software-defined vehicles.

Helping clients achieve **360-cybersecurity**, AUTOCRYPT's offerings include a wide range of custom solutions that ensure all vehicles are safe from both internal and external threats.

AUTOCRYPT's **proprietary technologies** establish cybersecurity by covering threat analysis and risk assessment, smart fuzzing, penetration testing, embedded security software, and much more.

Driven by two decades of experience and expertise in encryption, authentication, and intrusion detection and prevention, AUTOCRYPT offers end-to-end security for safer communications between road participants.

AUTOCRYPT

For more information about AUTOCRYPT's comprehensive security solutions,
visit **autocrypt.io**
For partnership inquiries and solution consultations,
contact **global@autocrypt.io**