

# Protection of Intellectual Property Rights in Automotive Control Units

Armin Wasicek  
University of California

## ABSTRACT

Intellectual property rights and their protection is a cornerstone of the automotive value chain. The automotive industry is composed by a meshwork of tightly integrated organizations that cooperate and compete in a hierarchical marketplace. Trading know-how and other virtual assets between participants is an essential part of this business. Thereby, software as a medium to transport ideas, innovations, and technologies plays a particular role. Protection of virtual goods and their associated rights is a current issue whose solution will determine how business will be done in the future automotive market. Automotive experts and researchers agree that ICT security technologies are a vital part to implement such a market. In this paper we examine the software life cycle of an automotive Electronic Control Unit (ECU) and discuss potential threats and countermeasures for each stage. In particular, we will look at the following threats: (1) development (leakage of know-how through insiders or industrial espionage), (2) production (leakage through split inventor/producer companies), (3) deployment and service (manipulation of ECUs), and (4) aftersales (combating counterfeit ECUs and spare parts). Next, we link our findings to the AUTOSAR methodology and life cycle model. Thus, we assess the state-of-the-art in automotive software development against the anticipated threats and countermeasures. As a result, we are able to propose improvements for the secure development and maintenance of software for automotive ECUs. Moreover, we are able to forecast the prospects of security technologies to protect automotive software.

**CITATION:** Wasicek, A., "Protection of Intellectual Property Rights in Automotive Control Units," *SAE Int. J. Passeng. Cars – Electron. Electr. Syst.* 7(1):2014, doi:10.4271/2014-01-0338.

## INTRODUCTION

The security of Cyber-Physical Systems has gained lots of attention recently. A number of spectacular hacks [7] and failures [4] contributed to make this field widely visible. Consequently, it has been acknowledged that security should be part of a well-designed product. Looking at current products, it turns out that many are actually vulnerable. The reason behind this circumstance is that in many domains, the goals of security systems are not as clearly defined compared to required fault tolerance capabilities. This again roots in the absence of *incentives* for companies to integrate security in their products. Making a strong business case for cyber security investments is difficult, because threats and risks are hard to predict, and consequences are hard to demonstrate. As a result, systems remain insecure.

This paper aims to put one major incentive for the automotive industry to implement security in their products on the table: the protection of IP rights. Currently, the automotive industry experiences a paradigm shift from mechanical and electrical systems towards software-driven systems. Alongside with this shift, global system architectures (e.g., AUTomotive Open

System ARchitecture (AUTOSAR)) are emerging that enable the exchange and increase the tradability of software products. The main contributions of this work are:

- Survey the existing trends in the automotive market and in automotive security,
- Relate these findings to the AUTOSAR methodology, and
- Propose Secure Software Envelopes as a security scheme for the exchange of software components in the future automotive market.

The next section gives an overview of the development of the automotive industry and its major stakeholders. Next, the paper discusses the role of Information and Communication Technology (ICT) security in automotive applications and aligns these requirements to the life cycle of an automotive product. Thereby, potential threats and countermeasures are considered. The next section briefly surveys current approaches to enable automotive security. As an example for an automotive system engineering approach the AUTOSAR methodology is presented next. After describing the state-of-the-art of security in AUTOSAR, the concept of Secure Software Envelopes is presented to facilitate the protection of Intellectual Property (IP) in the future automotive market.

## THE AUTOMOTIVE INDUSTRY

The automotive industry is currently undergoing a major paradigm shift. Throughout the 20<sup>th</sup> century the bulk of revenue were created by selling vehicles. The industry profited from the effects of mass production and industrialization. Delving into these effects led to an increasing volume of vehicles sold but also to diminishing returns per unit. This again triggered the ongoing consolidation process of the automotive industry that is still ongoing and will leave only a few global Original Equipment Manufacturers (OEM) and suppliers at the end.

Entering the information age in the 21<sup>st</sup> century opens new challenges and business opportunities in the automotive market. Relevant trends are shifting mobility needs, readiness of new information technologies, a global automotive marketplace, demand for high fuel-efficiency, safety, and driving experience. All these trends will fuel the emerging automotive business for the coming decades. In order to cope with these trends, the automotive companies will have to abandon their traditional business models and reinvent themselves being a high-tech, innovation-based industry. Newly emerging markets in China, India, grow fast and build up new companies and brands that push on the global market. The big high-tech companies<sup>1</sup> reach out to the automotive domain and develop new technologies that have the potential to revolutionize the automotive market.

Anyway, it is not yet determined what this new marketplace will look like and how to succeed. Transitioning to a knowledge-based society, one thing appears to be obvious: the automotive industry of tomorrow will reward innovation. Thus, generating and maintaining IP will be a key success factor. The protection of IP rights will be therefore not only a concern of laws and jurisdiction, but also a technological challenge.

### The Automotive Marketplace

Historically, the automotive industry roots in enterprises that produce for the domestic markets. Subsequent mergers, acquisitions, and specializations throughout the past 40 years structured the automotive industry in the current hierarchical system of OEMs and suppliers. These large-scale companies built up an international meshwork of tightly integrated companies and organizations. The consolidation process of the autom industry has not yet come to a halt. Starting with 36 car manufacturers in 1970, today there are 12 globally acting OEMs, each addressing the full range of vehicles [34]. Until 2020, the number will decrease to ten OEM groups that account for 90% of the sales in the six key markets in China, India, Western Europe, Japan, Korea, and the United States [10]

The consolidation propagates through to the supply chain .**Error! Reference source not found.** Figure 1 depicts this process. Through merging Tier-1 and Tier-2 suppliers a few global mega-suppliers, sometimes

referred to as “Tier 0.5 suppliers”, will emerge. This new class of supplier will have high competences with respect to the technical challenges of building a vehicle. Thereby, the suppliers' market share will increase to about 68% in 2015. For instance, such a supplier could deliver complete vehicle subsystems, for instance, a power train. OEMs, however, will take care of integrating the subsystems, producing a large volume series, giving the car its look-and-feel, as well as branding and advertising.

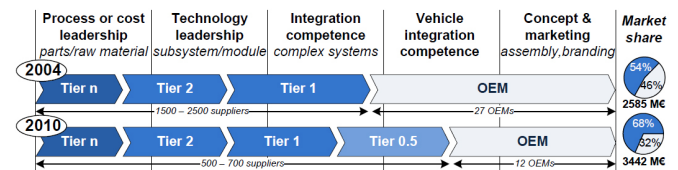


Figure 1. Automotive value and supply chain

Consequently, the consolidation process breaks up the vertical integration of the automotive industry. In each tier of the value and supply chain there will be less but more competitive companies. Each company will have its own specialization and business opportunities will be created by ‘mutualization’, for instance, to share investment and risk of new developments. In the high-tech industry, this way of doing business is already well established, for instance, Google invented the Android system; Samsung and other companies produce devices. Cooperation requires the partners to exchange know-how and IP. A key to success in the newly emerging automotive marketplace will be a company's ability to generate, maintain, and exchange IP, on the one hand to develop own products, and on the other hand to provide service to other companies.

In addition to the consolidation process, profit margins from car sales are decreasing, thus, abolishing the traditional business model of the OEMs. At the same time, the after-sales market is becoming an increasing important source of revenue. For example, in Germany the after-sales business generates more than half of an OEM's profits while accounting for only 23% of an OEM's revenues [14].

### Innovation Drivers

The newly emerging marketplace will be fueled by innovation. Potential areas for innovation include:

- **Shift from mechanical to electronic components:** X-by-wire, increased reliability through electronics, etc.
- **Driver assistance systems:** Autonomous Emergency Braking, Lane Assistant, crash prevention, etc.
- **Advanced energy management** in hybrid and Electrical Vehicles
- **Car-to-Infrastructure, Car-to-Car:** Information exchange between vehicles and their surroundings

Innovative ideas and concepts will be turned into components and control units on the supplier side. The city, car and road according to a German OEM – that electronics and software will

1. E.g., Open Automotive Alliance, Google Driverless car,

make up 75% of all future innovations [13]. The percentage of production cost of electronics reflects the rising importance of Electronic Control Units (ECU) in vehicles: it increased from 19% in 2004 to 40% in 2010 and it will eventually reach 50% in 2020 [34]. It is getting a commonplace knowledge that cars will be future software platforms, much like telephones nowadays.

### Intellectual Property Rights

Trading know-how and other virtual assets between participants in the automotive marketplace is an essential part of this business, particularly when dealing with electronics and software. Software is an excellent medium to transport ideas, innovations, and technologies. A software program can implement a prototype, model a technical process, or represent a technology. The expressiveness and formalisms of computer languages allow to conceptualize and to execute ideas at the same time. This is what makes software such a valuable tool for systems engineering.

Functions that are commonly implemented in a vehicle's software are, for instance:

- **Control algorithms** that drive the car and give it its sensation: engine control including hybrid power distribution, predictive control to enhance performance and efficiency.
- **Safety functions** like Anti-lock Braking System (ABS), or Electronic Stability Program (ESP), etc.
- **Driver assistance systems**, e.g., navigation, obstacle warning, road status assessment to record and present information like traffic signs, lane to the driver.
- **Infotainment systems** like radio, TV, etc.
- **Diagnostic systems** that report the vehicle's current status to the driver and maintenance engineers, either locally via dashboard and onboard diagnostic interfaces, or remotely via a web interface.

The software programs for these system functions are mostly implemented in a distributed manner. Thereby, several ECUs communicate over a vehicular network like CAN, FlexRay, or MOST, or Ethernet. A company's assets may be the software implementing the actual system function, middleware implementing some non-functional properties (e.g., reliability, availability, security), tools and procedures to derive these programs from higher-level models, or to translate program code to machine code. The production and distribution of these virtual goods is part of the business model of many suppliers. Other business activities include services like testing, calibration, consulting, manufacturing of hardware units, sensors, and actuators.

Traditionally, ECU and software have been considered as an integral unit of assembly in the automotive domain. Up to now, the role of software was rather that of a side-product that is required to make the ECU function in a desired manner. Software was traded together with an ECU as a functional unit. Thus, engineers focused rather on assembling physical

devices than on integrating several software products. Currently, there is a shift to separate software and ECU. This development reflects a major step beyond the state-of-the-art in automotive engineering.

The envisioned software can be subdivided into modular building blocks, namely Software Components (SWC) that are *integrated* in an ECU. The actual code inside an ECU is thus often produced in collaboration of several suppliers. In order to produce its share of the code, a supplier must develop, test, and integrate against the software components of other suppliers. Since the components are the IP of their respective suppliers, the suppliers might not be willing to share with their collaborators who might be competitors in the next project. Consequently, suppliers do not share their actual code, but rather exchange black box models consisting of interface specifications of all the incoming and outgoing signals. SWCs are anticipated to be a basic unit in future automotive architectures. Adhering to a particular architectural style therefore opens a market for an OEM or supplier.

Moreover, some SWCs will become a commodity in the automotive market [26]. For instance, a CAN driver looks very much the same, whether company A or B delivers it. The goal of a control algorithm for an ABS system is similarly clear. How well it fits into a particular vehicular platform might differentiate suppliers. Being a commodity means that similar products are available that differ only in quality and price:

*"Commodity is defined as a product or a set of goods, which has a constant demand and is supplied 'without any qualitative differentiation' within a market. This product remains the same no matter who manufactures/develops/produces it. Some examples are steel, milk, paper, pencils etc. The price of this product is typically a universal constant but it fluctuates based on global supply and demand. There could be variants to the product but it is important to note that these are well-defined and bounded in terms of specifications."* [26]

Software, on the contrary to physical items such as steel, milk, paper, etc., has, after development, an extremely low production cost (i.e., copying). This principal attribute of software is both blessing and curse at the same time; the availability of production and distribution facilities is not an entry barrier for new competitors as, for instance, in the steel market where new entrants require a steel mill for production. However, the functional part of the software cannot distinguish, if it is an authorized copy or not. Enforcing the notions of *authentication* and *authorization* for automotive software is one major goal for automotive security systems.

IP rights are associated with all virtual assets in order to enable business between companies. Regulations, however, are a necessary means to constrain the market and to enforce rights and duties (e.g., warranties, liabilities, remedies) associated with the ownership of these assets. As the automotive marketplace takes place globally, these regulations might not be always enforceable by jurisdiction, simply because the legal

systems in the six automotive key market areas are not yet as compatible as it would be necessary. Moreover, the connotation of the term 'intellectual property' is subject to cultural differences. Digital ownership is far from being clearly and commonly agreed concept. The discourse is ongoing [30]. In this area of conflict, ICT security is an enabling technology for the emerging automotive marketplace. Regulations alone will not suffice to match the challenges of the future automotive market. ICT security can be used to support and monitor regulations. As a basic function it can be used to implement digital ownership protection. A secure automotive market will be open for new companies (e.g., from the high-tech industry) and at the same time protect rights of established participants.

### The Role of ICT Security

Protection of virtual goods and their associated rights is a current issue whose solution will determine how business will be done in the future automotive market. Automotive experts and researchers agree that ICT security technologies are a vital part to establish such a market [38] [21]. In automotive engineering, there are several security objectives that would require deploying ICT security technologies:

- **Tamper prevention, response, and evidence:** A vehicle's computer system has to be *protected against unauthorized actions* from users (e.g., car owners), maintenance engineers (e.g., unofficial garages), etc. A particular concern is the *propagation of a security breach to the safety domain* (e.g., a car tuner who modifies the engine controller's control algorithms) [36]. Tamper prevention, response and evidence are different escalation levels for security mechanisms. The main security goal is to improve the ECU's resilience by protecting the vehicle from unauthorized modification and manipulation.
- **Copy protection:** ECUs contain software that is proprietary to the OEMs or their respective suppliers. The software programming represents a major effort and the software itself can contain IP in form of novel (control) *algorithms, parameterizations*, etc. Copy protection mechanisms secure this software against unauthorized readout, transfer, and other modes of usage beyond the according license. ICT security is employed to counter disclosure of sensitive programs.
- **Digital Rights Management (DRM):** Vehicles use increasingly *digital content* from third parties like entertainment (e.g., music, movies), maps for navigation systems and apps. This connects the automotive domain to other digital marketplaces that have their own code-of-conduct and legal systems. The vehicle's interface to these content providers must implement the required security standards to access these rich content sources. Security properties like accountability, confidentiality, and authentication form the basis for DRM.
- **Liability:** As most ECUs represents a collaborative effort of different suppliers and on or more OEMs, the question of who has to assume *legal responsibility* for a malfunction

or a failure, has often no clear answer. The integration of different software components onto a hardware platform is a challenging task that takes lots of engineering effort. Side effects from the integration and lacking unambiguous diagnostic functions make it difficult to assign a failure and therefore the provision of the required corrective measures to a single collaborator. Establishing trust during the integration process and installing mechanisms to verify accountability are potential security goals to reach this very sensitive security objective.

- **Enabling new business models:** As the automotive market is changing, new software-based business models will emerge. *Personalization* is one example for such a technology-driven business model. In this model, an ECU's software contains besides its basic function some additional functionality (e.g., convenience or premium functions) that can be enabled/updated based on a fee. Other examples are *location-based services* and *aftermarket software* sales. Authentication plays a major role to distinguish authorized and unauthorized users.
- **Theft prevention:** This is the classic ICT security application field of the automotive domain. Electronic immobilizer systems successfully reduce car thefts [25].

ICT security solutions must not only be implemented by software means, but they have to root in the ECU's hardware. Software offers application designers a tremendous flexibility to design, implement, and maintain their products. These benefits, however, entail certain drawbacks. Software offers no inherent mechanisms to protect itself from unauthorized modifications or illegal copies. Protection of software usually requires at least minimal support from the hardware in order to establish a root-of-trust [33].

Security solutions must not only be technically secure, but they address a multi-dimensional problem involving technical, social, legal, political, and commercial issues. They have to be organizationally feasible and aligned to the life cycle of a product. This makes the design, implementation, and maintenance a tough challenge that requires a considerable engineering effort. In the past, security has often been treated as an add-on and been introduced very late in the software development process. Moreover, the *penetrate-and-patch* [23] approach, which is very common for standard IT systems, is not feasible in a CPS. A running CPS might not be easily stopped, because it involves physical processes that might have a long response time and might not be easily halted. For instance, halting an engine controlling ECU because of an intrusion can ultimately lead to stopping a vehicle, which might not be in the best interest of the user.

Automotive software engineering [28] is a complex process that requires many different skills, tools, and know-how to succeed. It is nearly impossible (and might also be inefficient) for a single organization to cover all different aspects of this comprehensive, multi-disciplinary task. Suppliers and OEMs collaborate on many different levels to derive a product. For