Study on the Advanced Driver Assistant System

Annapoorani.M¹, Dheleep Kumar.C², Jaikrishna.S³, Yaswanth Arvinth⁴.

Students ¹,²,³,⁴

Department of Electronics and Communication Engineering

Coimbatore Institute of Engineering and Technology

Abstract—Vehicle automation started many years ago (engine control, automatic starter, ABS, ESP, ...) and more recently the development of Advanced Driver Assistant System (ADAS) has generated a real technological break. ADAS have the potential to optimize safety and efficiency in road traffic. The main objective is to clarify the goals and guidelines for future development in the area of advanced driver assistance systems (ADAS).

Introduction

This paper discusses security vulnerabilities and potential solutions for Advanced Driver Assistance Systems (ADAS). We introduce ADAS system architecture and present use cases. We further provide detailed threat analysis of two leading ADAS use cases: (1) lane departure warning and (2) adaptive cruise control. Based on threat analysis results we identify security problem areas and state security requirements for each. We devote the last part of this paper to ADAS security solutions that can meet identified objectives. This study makes several key contributions to addressing ADAS security problems:

• Establish critical needs to addressing security problems via detailed threat analysis
• Define main security problem areas for ADAS
• Identify challenges and requirements for securing ADAS control functions
• Establish the mission of securing E2E ADAS data path
• Define trust foundation for secure ADAS platforms
• Make recommendations for “ADAS security solution menu”

There are several challenges to design, implement, deploy, and operate ADAS. The system is expected to gather accurate input, be fast in processing data, accurately predict context, and react in real time. And it is required to be robust, reliable, and have low error rates. There has been significant amount of effort and research in the industry to solve all these challenges and to develop the technology that will make ADAS and autonomous driving a reality.

In addition to functional requirements, ADAS must be secured from adversaries with malicious intent whose goal is to compromise the system and cause catastrophic accidents with loss of life and damage to property.

It has been shown both in academia and automotive industry that control system can be compromised via malicious attacks launched through various means, for example via DVD player, the ODB-II port, or even wirelessly via tire pressure sensors as a result displaying to the driver wrong warnings or even causing fatality by remotely disabling braking system on a vehicle while it is moving.

In addition to protecting the system from criminal actors, there is a bigger threat looming from nation-state sponsored cyber terrorism.

In this whitepaper we argue that ADAS security should be considered as a fundamental non-functional requirement— together with reliability, robustness, performance, and low error rates. We analyze vulnerabilities in a conceptual ADAS architecture via representative use cases. Based on the vulnerability analysis results we state security requirements and make suggestions on countermeasures against malicious attacks. We show that ignoring ADAS security compromises other design goals.

ADAS System Background

ADAS system provides assistance to the driver and improves driving experience. Its primary function is to ensure safety of the vehicle, the driver, and the pedestrians or bikers. ADAS could be used to save fuel costs by enabling platooning in which vehicles follow each other within close distance; it could warn when a vehicle swerves across the lane or it could apply emergency brake to avoid collision. To function reliably, ADAS must be able to recognize objects, signs, road surface, and moving objects on the road and to make decisions whether to warn or act on behalf of a driver.
ADAS Example Usage Cases

ADAS system is considered as the advancement from driver assistant system (DAS). DAS is a system that informs and warns, provides feedback on actions, increases comfort, and reduces workload by actively stabilizing or maneuvering the vehicle. ADAS system is considered as a subset of DASs, with increased use of complex processing algorithms to detect and evaluate the vehicle environment based on data collected via a variety of sensor inputs. Figure 1 demonstrates the spectrum of DAS capabilities available in production today; the capabilities considered as ADAS are highlighted with stars. The ADAS usage cases that require full power of real-time processing and intelligence are highlighted with full stars, whereas half-colored star marked usage cases are relatively more rudimentary ADAS cases.

ADAS Conceptual Architecture

To support ADAS functions the architecture must include modules for sensing, processing, intelligence generation, and decision making. Figure 2 is a generic view of what the ADAS system might look like. The overall system compromises sensors of various types; a CPU-GPU combination to perform the sensor data processing, object identification, and early sensor fusion; a “Central Brain” CPU for performing sensor fusion from different sensor blocks.

NEED FOR ADAS

ADAS is a vehicle control system that uses sensors to sense the parameters such as line change, collision avoidance, fuel level detection, etc. To give comfort to the driver. This will make the driver comfortable during driving as he will be able to Recognize as well as control during traffic situation. Driver information system increases the driver's situation awareness and driver warning system actively warn the driver of a potential danger e.g. lane departure, Blind spot, low light intensity, obstacle in the path. According to several surveys ADAS can prevent up to 40% of accidents, depending on the type of ADAS used and the type of accident. The overall objective of this project is “to determine the Requirements and design standards for a class of intelligent driver support systems which will Confirm with the information requirements and performance capabilities of the individual drivers”.

ADAS Security Problem Areas

Before looking into details of security threats, let us first examine, at high level, what are the major areas of concerns for ADAS system in dealing with hostile running environment and malicious actions by adversaries. In general, any malicious actions that could cause ADAS system to behave outside its specification are referred to as threats to ADAS. And the interfaces that allow such threats to occur are referred to as attack surfaces. Now the key questions are: what is the specified behavior of an ADAS system, and how do attackers cause the system to misbehave? The answers to these questions lead to the discovery of three major ADAS security problem areas.

Crashes Survey

Study shows that due to road accidents around 1.2 million deaths are taking place around the world. Table 1 shows crash survey due to various factors. Accidents are taking place due to issues such as traffic congestion, rash driving and lane change over. The intelligent driver assistance system provides solution to such problems by supplying automatic controls and slows down or stop the vehicle under emergency. This system monitors distance between a moving vehicles, monitors level of petrol, monitors obstacle. ADAS are systems to help the driver in the driving process. Driver assistance system enables safe, relaxed driving, based on intelligent sensor technology.

| S.no | Crashes due to various factors                  | Percent |
|------|-----------------------------------------------|---------|
| 1    | Driver factors                                | 57%     |
| 2    | Poor visibility                               | 27%     |
| 3    | Vehicles problems & driver factors            | 6%      |
| 4    | Roadway factors                               | 3%      |
| 5    | Roadways & driver & vehicle factors           | 3%      |
| 6    | Vehicle factors                               | 2%      |
| 7    | Roadways & vehicle factors                    | 1%      |

Adaptive cruise control system

An ACC controller must be tested in a closed-loop experiment, since the ACC control actions affect the relative motion, which in turn is detected by the environment sensor. Apart from the vehicle itself, optionally a human driver can be included ‘in-the-loop’ to operate the ACC control lever and...
introduce disturbances. The prototype vehicle has been implemented with the feedback control law
\[ ad = -k_1 \cdot x + k_2 \cdot v, \quad k_1, k_2 > 0, \quad (27) \]
to obtain a desired acceleration \( ad \) that controls both \( ex \) and \( vr \) to zero. In order to achieve a natural following behaviour, the desired clearance is chosen as \( xd = \max(\nu \cdot 2 \cdot h, x_0) \) and the feedback gains are calculated by nonlinear functions \( k_1 = f(v_2, x, \nu, h, \nu_0) \) and \( k_2 = f(v_2, h) \), where \( x_0 \) is a distance safety margin and \( h \) is the driver-selected time gap.

Control law (27) is tested for the traffic scenario of figure 10: the ACC-equipped vehicle 2 drives on the middle lane when suddenly another vehicle 1 cuts in from the right lane at a lower speed (\( vr < 0 \) and \( ex > 0 \)). This happens at \( t = 22.9 \) s, which can be seen from the range \( x_r \) and angle \( f \) to the target. As soon as the radar sensor on vehicle 2 detects the obstacle in its lane (i.e., \( f = 0 \)), (27) gives \( ad < 0 \) and the ACC activates the brake system at \( t = 25.3 \) s. Vehicle 3 stays on the right lane and is used to test the ability of the radar to distinguish between important and irrelevant targets in the traffic environment (i.e., vehicle 3 should not be considered a target). On a test track it would be very difficult to safely and reproducibly carry out such a test with human drivers, but in VEHIL the scenario can be accurately reproduced. Especially note the transformation from absolute to relative motion, i.e., \( v_{mb} = v_1 - v_2 \).

The results also show that the MB has a maximum error \( e \) of 0.10 m between desired and measured position, and a reproducibility within 0.01 m between consecutive test runs.

The velocity error is usually smaller than 0.1 m/s. This dynamic accuracy is reached up to a bandwidth of 5 Hz and a velocity of 50 km/h, and is within the measurement noise of any automotive environment sensor. Similarly, the chassis dyno can be accurately controlled up to a bandwidth of 5 Hz.

With these type of tests VEHIL has an added value in identifying the requirements and capabilities of an ACC system for safety-critical traffic scenarios in an early development stage. Using rapid control prototyping techniques, various control settings are efficiently tested for a variety of scenarios. When the effect of various traffic disturbances on control performance is known, controller parameters can be optimally tuned. In addition, in a later stage functional validation of the completed system to these requirements can be done unambiguously and efficiently.

**Forward collision warning system**

Testing an FCW system is more safety-critical than ACC, since a collision warning system is activated shortly before a collision is expected. A warning is issued when a threshold of maximum braking capability \( a_{2,min} \) is crossed by the required deceleration \( ad \) to prevent a collision. The algorithm takes into account whether an initially moving lead vehicle (i) stops prior to the following vehicle, or (ii) is still in motion when the host vehicle stops.

Taking into account driver reaction time \( f \), \( ad \) is given by
\[ ad = a_{1 \cdot v^2} / 2a_1((v^2 - x + s_0) + v_2), \quad \text{case (i)} \]

\[ a_{1 \cdot v^2} - 12/2a_1(12v + v_2) + x - s_0, \quad \text{case (ii)} \]
such that a collision is avoided by a safety margin.

The truck is equipped with a control law similar to (including some nonlinear characteristics). In the simulated scenario, an inattentive truck driver slowly closes in with 25 m/s on another vehicle driving at 23 m/s (represented by the MB). After the preceding vehicle suddenly brakes at \( t = 46.7 \) s, \( ad \) in (28) drops below \( a_{2,min} \) at \( t = 49.2 \) s, and subsequently the FCW system sends a collision warning to the driver. The corresponding test results in figure 14 show that, after a slight delay due to driver reaction time, the driver brakes at \( t = 49.9 \) s and avoids the collision. In this way, optimum warning thresholds are defined by executing reproducible and safe experiments. Apart from objective parameter tuning, VEHIL also seems to have potential for subjective evaluation in addition to on-road tests. It can be verified whether the warnings, when given in defined critical situations, are adequate. Although the final subjective evaluation should be done on the road, VEHIL can be used for an initial evaluation.

Furthermore, ongoing research focuses on validation of VEHIL test results with test drives and Development of advanced driver assistance systems.

**Challenges in the ADAS development process**

The ADAS development starts with a definition of the functional requirements in terms of the desired functions, driver comfort, and operational constraints. In addition, ADASs are safety-critical systems that require a high level of dependability, a term covering reliability, (fail-) safety, and fault-tolerance. Hazard and risk analyses are therefore performed to identify the safety requirements, usually in terms of the rate of false alarms (when an ADAS takes unnecessary action) and missed detections (when it fails to correctly detect a dangerous situation). State-of-the-art systems achieve a false alarm rate in the order of 10⁻⁵ per km, but this is still considered too high [12]. From the functional and safety requirements a system specification is produced to define the precise operation of the system. However, in practice requirements are often difficult to define and subject to ambiguity, which may lead to an incomplete or incorrect specification. Subsequently, the system specification is used as the basis for the top-level design of the system architecture, followed by detailed module design (environment sensor, controller, actuator, driver interface). After implementation of the individual hardware and software modules, system integration takes place by assembling the complete system from its component modules. In every integration phase verification takes place to determine whether the output of a phase meets its specification, as illustrated by the horizontal arrows in figure.

On component level this means testing the range, accuracy, and tracking capabilities of the environment sensor. On a higher level, verification must assure that integration with other subsystems does not have any negative side-effect. Since verification only confirms compliance with the
specification, errors in the specification may result in a faulty product. It is therefore important to perform validation of the integrated system against its requirements, especially for type approval and certification purposes. Usually, the development process involves several iterations, where the results of verification and validation are used to modify the system specification and design, after which another test cycle takes place. Obviously, there is a need to reduce the number of iterations and speed up the process of verification and validation. Because of the need for fast, flexible and reproducible test results, various ‘in-the-loop’ simulation tools are increasingly being used for design and validation of ADAS controllers, as indicated in figure 3. After a review of these tools, the position of the new VEHIL simulation tool in this development process will be clarified.

References

[1] Akira Jinoshi,”Driver assistance (lane keep assist system)”, Presentation to WP-29 ITS Round Table Geneva, 2004.
[2] Daniele Bagni, Roberto Marzotto, Paul Zorath,”Building Automotive Driver assistance Algorithm with Xilinx, FPGA platforms.”, Xcell Journal Fourth Quarter 2008.
[3] Hella KGaA, Hueck & C0,”Electronics Driver assistance system”, technical information, 2005.
[4] Huei Peng,”Evaluation of Driver assistance System- A Human Centered Approach “, supported by the U.S. army TARDEC, NSF & TRW Automotive, 2006.
[5] D De Waard, T.G.M.P.R. Van den Bold,&B Lewis-Evans”Driver hand position on the steering wheel while merging into motorway traffic,” Transp.Res, part F, Traffic Psychol, Behaviour vol 13,no2, Mar 2010
[6] Surawanan Kunan, Arunkumar Thangavelu, Ramesh Babu Kalivaradhan,”An Intelligent Driver Assistance System (I-DAS) for Vehicle safety modeling using ontology Approach”, International journal of UbiComp (IJU), vol.1, No.3, July 2010
[7] Steven S. Beuchemin, Michael A. Bauer, Taha Kowsari, Ji Cho, ”Portable snd scalable vision based vehicular instrumentation for the analysis of driver intentionally”, IEEE transactions instrumentation And measurement, vol.61, No.2, FEB 2012
[8] Bo Wu, Ram Nevatia. Detection of Multiple, Partially Occluded Humans in a Single Image by Bayesian Combination of edgelet Part Detectors. Proceedings of the Tenth IEEE International Conference on Computer Vision (ICCV’05) 2005.
[9] Xiaodan Wang, Chongming Wu, Chunying Zheng, Wei Wang. Improved Algorithm for Adaboost with SVM Base Classifiers. Proc. 5th IEEE Int. Conf. on Cognitive Informatics (ICCI’06) 2006; 948-952.
[10] M. Bertozzi, A. Broggi, C. Caraffi, M. Del Rose, M. Felisa, G. Vezzoni. Pedestrian detection by means of far-infrared stereo vision. Elsevier Computer Vision and Image Understanding 2007; 106:194–204.
[11] Stephen J. Krotosky, Mohan Manubhai Trivedi. On Color-, Infrared-, and Multimodal-Stereo Approaches to Pedestrian Detection. IEEE transactions on Intelligent Transportation Systems 2007; 8-4: 619-630.
[12] Liping Yu, Wentao Yao, Huaping Liu, Fasheng Liu. A Monocular Vision Based Pedestrian Detection System for Intelligent Vehicles. IEEE .

@IJRTER-2018, All Rights Reserved 166
