IoT4CPS
Trustworthy IoT for CPS

Autonomous Driving: Safe and Secure Automated Driving Platform

Challenges, Technical Solutions & Application Use-Cases

Date: November 2020
Editor: Andreas Eckel
Authors: Edin Arnautovic, Andreas Eckel, Stefan Jaksic, Thomas Mauthner, Omar Veledar

Contents

1. SUMMARY

The goal of this document is to introduce IoT4CPS achievements in terms of use-case applications in Automated Driving (AD). To that extent, the focus is placed upon the needs for such development and implementation of a secure platform for automated driving, as well as the deployment of such platforms. The demonstration is two-fold. One aspect covers showcasing the results in a controlled reduced scale environment (rover robot), while another aspect touches upon implementation in a real vehicle, still in a controlled environment.

To achieve feasible demonstrations with a realistic exploitation potential, the demonstrations are engaging the technological advances that are resulting from IoT4CPS activities. These are combined with the assets and expertise of project partners to realise integrative solutions with marketable potential. The resulting demonstration is contributing to answering some of the aspects of the given challenge. The main benefits are seen in improvements in road safety, increased driving comfort and improved mobility options. All in all, the offered solution is simply a step forward in the quest to increase driving automation level. The key interest of relevant stakeholders goes beyond reaching the appropriate functionality and includes the development of secure solutions that are resistant to cyber-attacks. Such accomplishment would create an undoubtful benefit of protecting the relevant data from unscrupulous unauthorised behaviour, while also safeguarding the safety aspect of AD. The nature of the application creates a tight and inseparable link between IoT security and safety of the road users. On the whole, the trustworthiness of the offered dependable solutions is the key target, which is essential for increasing user acceptance levels towards AD.
To reach the high dependability level, the technological advances and their integration must undergo a double conceptual shift. The first shift is related to departure from the fail-silent ADAS features and the move towards fail-operational AD deployment. Another shift is the one that departs from the existing usage of dedicated ECUs for each feature towards consolidated central control. Both of those are dependent on sensor fusion and edge AI methods, which are outside of the project's scope.

The use case demonstration presented in this document is based on considers the integration of a secure and safe development platform into a rover robot and testing of certain AD functionalities. Aside from the validation and verification aspect for the SW functionality, the demonstration offers the possibility for experimentation with a range of sensors that could be suitable for future driving applications. Another demonstrator considers the integration of a generic platform for development, validation and verification of AD functionalities in real driving conditions. The security aspect of the associated connectivity solutions is assessed and recommendations are provided for future applications.

2. CHALLENGE

2.1Current Development Targets in the Automotive Industry

The present automotive megatrend of driving automation [Schramm, 2013] is a substantial contributor to the Grand Societal Challenges. The highly automated driving functions provide the following societal benefits:

- Increased road safety through reduced human influence, as many accident-causing factors are due to human errors [Eichberger, 2011].
- Increased driving comfort ranging from automation of routine tasks (vehicle guidance in traffic jams) to the usage of time spent in the vehicle for other activities.
- Facilitating mobility in old age by the supportive effect of automated driving, which is becoming a necessity driven by demographic changes [Reddy 2006].
- Enabled automated longitudinal-dynamic guiding behaviour to be better adapted to surrounding traffic and thus enable a reduced distance to the vehicle ahead (utilization of the slipstream may cause a significant reduction in fuel consumption) [Alam, 2010]
- More efficient utilisation of the road network by the implementation of platooning to shorten transport times (i.e. reduced driver resting period) [Bergenhem, 2012]
- Create an enormous potential for growth in the automotive industry for suppliers of electrical and electronic components and units/modules [Berger, 2016].

High level of vehicle automation demands full awareness of vehicle external environment, with 360-degree vision and peerless driving skills. Vehicle automation is in the focus of major OEMs and their market realisation is feasible by the end of the decade. On the path to that goal, the milestone of integrating Advanced Driver Assistance Systems (ADAS) into series production vehicles is already reached. Their limited automation (SAE level 2) does not relieve the driver from responsibility for the vehicle operation. Nevertheless, these ADAS functions, such as “Adaptive Cruise Control” or a “Break Assistant”, are paving the way towards passing on the driving responsibility from the driver to the automated driving function, hence turning the driver into a passenger. The anticipated commercially available SAE level 3 vehicles will take over the full driving function in certain driving scenarios. One of those is a “Highway Pilot”, which takes over the driving function up to a certain speed (i.e. up to 60 km/h to be used in traffic jams on highways only). Such vehicle prototypes, even in production-ready qualities, are already available and are in test phases, as well as in the process of achieving their approval for commercial sale and use. Prototype vehicles of a higher level of automation have been tested on public roads in Europe, Japan and the United States. These technologies have rapidly entered the market of premium cars and their future deployment is expected to accelerate. Many core technologies required for fully autonomous driving are mature enough for integration into commercially available vehicles. Others require further development in areas such as cyber-security. There is a need for additional measures to protect vehicles against unauthorized access to the control systems. Provision of required technologies to enable mass-market deployment of automated and context-aware vehicles demands major investment to foster innovation in simulation and validation environments, as well as

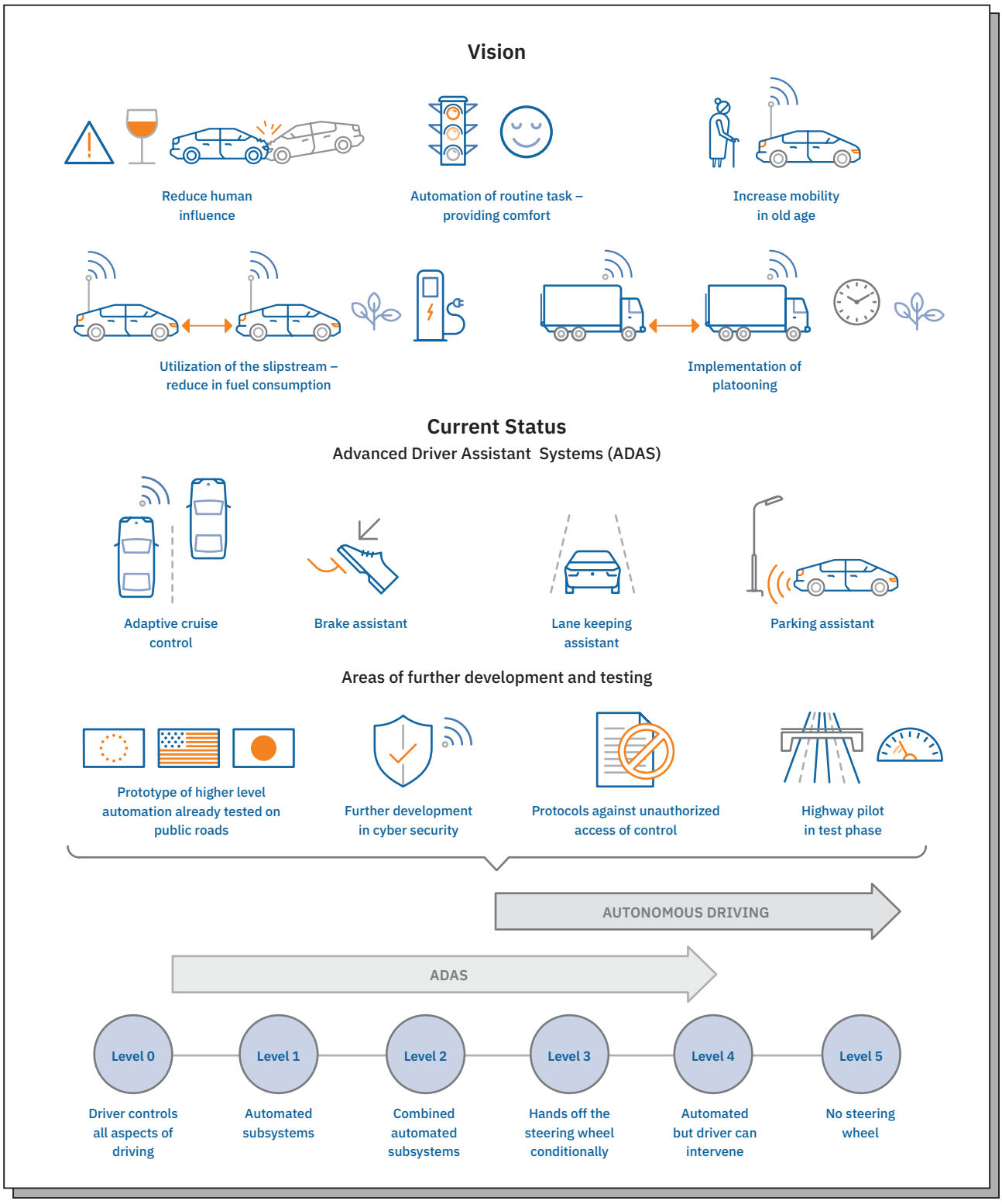

Figure 1: Current status and vision of the societal benefits provided by the highly automated driving functions

homologation concepts. Generally accepted, yet ambitious, estimates proclaim for level 3 automation to be reached in 2025+ and for level 4 and 5 is 2030+. The legislative updates are also needed in order to create a legal framework for operating highly automated driven vehicles in public space. SAE J3016 identifies six levels of driving automation from “no automation” to “full automation” (*Figure 1*).

2.2 Secure IoT for Automated Driving

An increasing number of vehicles is being connected to either the outside networking infrastructure or the Internet. It is a common understanding that “the connected car could be a cybersecurity nightmare” [CCR 2016]. Hackers have already broken into vehicles, taking over their functions and were able to gain control [Andi Greenberg, 2015]. Until recently, electronic automotive systems have been isolated from the outside world and the security was not deemed as a key challenge. Aiming at higher automation or even autonomy, the web connection and related security aspects become a necessity. Any digital system, which is integrated into connected vehicles, might represent a weak link and pose a security risk. Today’s connectivity mostly concerns non-safety-related functions, such as infotainment or navigation, which are becoming highly safety-relevant in highly automated driving. On the contrary, control functions of the future automated vehicles will be susceptible to the information from the infrastructure or other vehicles e.g., breaking or steering is affected if information about an emergency stop of one vehicle is transferred in real-time to other vehicles, which then can react much earlier than an average human driver. The full connectivity is also required to support OEMs’ intent to perform remote software updates for vehicle applications via internet links. Thus, the next generation of connected and automated vehicles exhibit an intricate interference between security and safety properties, e.g. through their distributed architecture and extensive use of data exchange and data analytics services. In simple terms, an highly automated and connected vehicle must offer safe behaviour, even if it is under adversary attack. First approaches towards safety and security co-engineering, SAE J3061 “Cybersecurity Guidebook for Cyber-Physical Vehicle” was published in 2016 and contains a proposal for co-engineering and automotive cybersecurity on a process and high-level requirements. Bringing this vision into practice demands wast additional research.

The shift from „fail-silent“ to “fail-operational” systems (as necessary for the highly automated driving on SEA levels 4 and 5) could potentially benefit from the experiences gained in the aerospace industry. This industry has already achieved significant advances in automation and near-autonomous or even autonomous operation. The ongoing research that targets appropriate redundancy concepts is considered as the key solution, but is yet to be perfected to the acceptable level needed for full marketisation. However, the price to be paid to apply this in safety-relevant concepts based on “dissimilar designed” and “triple redundant” systems is too high for automotive applications (i.e. highly automated driving). Consequently, there is a strong industrial pull of the inexpensive technologies and solutions that are also adequately fulfilling requirements. Virtualization and local clouds are currently considered to provide the most powerful and promising candidates to fulfil such requirements. Virtualization and centralization of control (Domain controllers or central controllers) will allow reduction of redundant units and will decrease the complexity of the resulting systems.

3. CURRENT STATUS

The vehicles, which are currently available on the market, are already equipped with quite sophisticated ADAS solutions. These are mainly built into the premium vehicle segments. These ADAS systems range from parking assistance, adaptive cruise control systems, braking assistants, lane-keeping assistants etc. Adaptive cruise control is capable of interfering into braking and accelerating a vehicle and can brake the vehicle automatically in case of an obstacle or a slower vehicle being detected ahead. Braking assistants also support the driver by automatically braking in case of obstacle detection. So far, the adaptive cruise control is a combination of the brake assistant and the static cruise control, which is capable of constantly keeping a certain speed level. The driver is still responsible for vehicle operation, but the automatic system takes over the speed control. The diver can overrule such SAE Level 2 system. Currently, there are no SAE Level 3 vehicles available for purchase. The first systems are out in test phases and are ready for sale in terms of quality and maturity. However, the homologation and thus the clearance to roll out such systems to the market are yet to be secured. The remaining issues range from requesting more redundancy up to security questions and insurance issues (who is liable in case of an accident “caused by the system”?). From single ECU towards “Domain Controller” targeting “Centralized Control”: The integration of technology developed in IoT4CPS aims to respond to the captured requirements including considerations for potential business cases and business needs in the area of highly automated driving. Detailed documentation is provided in deliverable D2.1, which argues the needs of the state of the art future developments needed to cover the issues of a “safe and secure platform” for highly automated driving. The increasing automation is heavily relying on senor information to produce the needed level of accuracy of environmental awareness. While for a long time each sensor was connected to its own ECU, designers are aiming to implement centralized architectures (*Figure 2*).

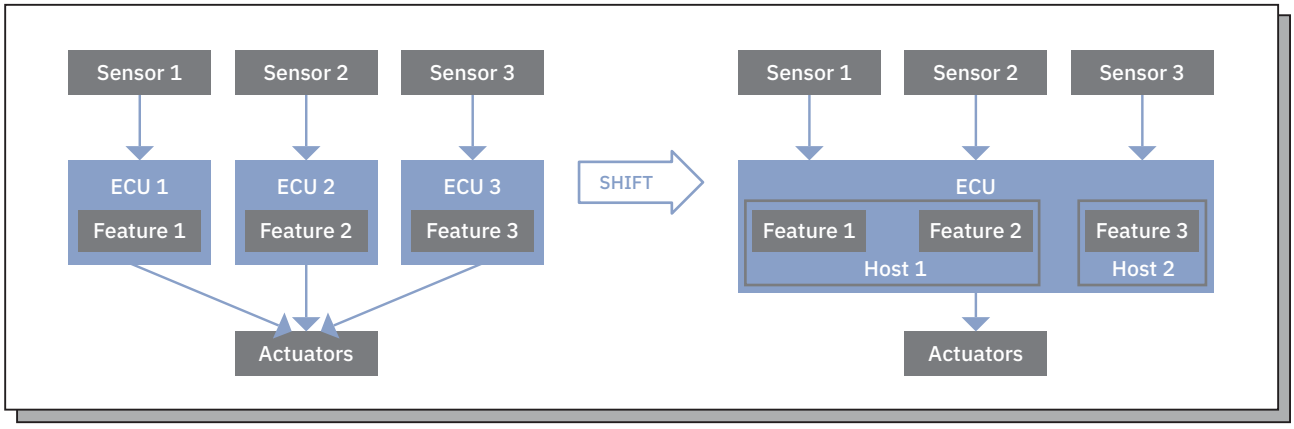

Figure 2: System architecture using (left) dedicated ECUs for each feature and (right) central ECU consolidating all features

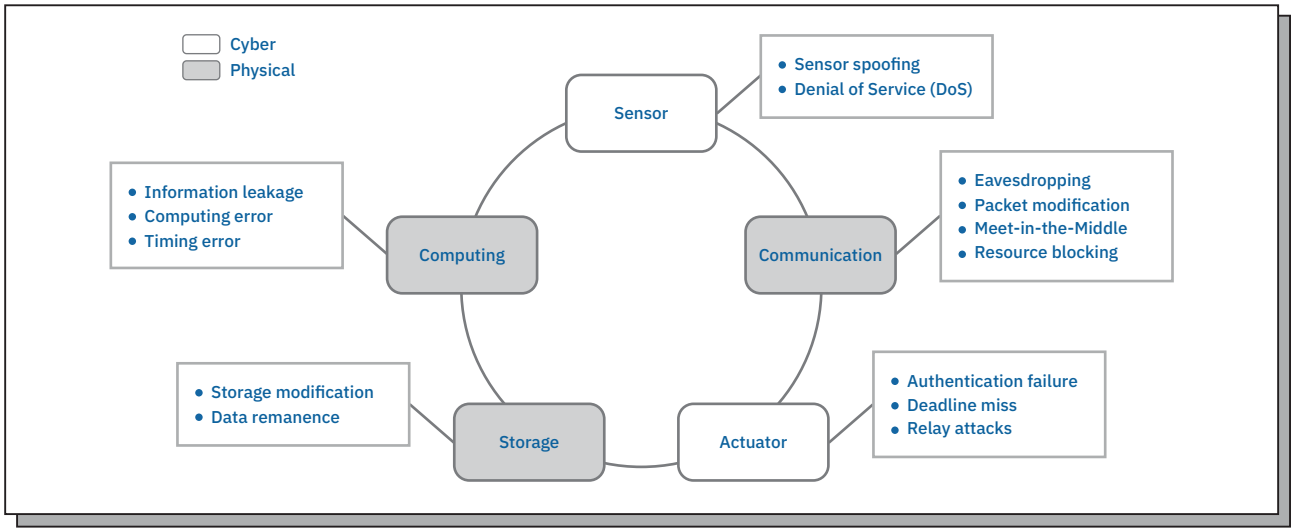

Figure 3: Attacks on IoT Systems

From “no Security Measures taken” towards “Security as a Safety Requirement”: In addition to the direct safety needs and the requirement to richer specifications and higher sophisticated applications with high computing performance needs, the request for including security measures also as a safety requirement. This goes hand in hand with the progressing connectivity also to the Internet that opens the gate for attackers (*Figure 3*).

On the other hand, the updates of software building blocks and modules by the manufacturers over the Internet is a too tempting feature to omit because of security/safety reasons. Furthermore, progressively more vehicles are destined to rely on the same hardware for a lengthened lifetime but will require software updates. In future, also Artificial Intelligence (AI) and Machine Learning (ML) modules will be integrated into the system. These algorithms also demand access to external computing power to process the collected information forming AI/ML-based software components. Such functionality is crucial for applications that rely on federated learning.

4. IOT4CPS TECHNICAL SOLUTIONS

4.1 Safety platform

From the functional perspective the AD systems contain multiple functions that demand usage of different properties from the underlying hardware and software platform. Figure depicts a high-level AD System Architecture which is mapped to a concrete safe and secure platform (TTTech) by the allocation of functions to hardware components. Sensor data (from radars, Time-Of-Flight (TOF) cameras, LIDARs, etc.) is integrated using sensor fusion to create a model of the environment (static and dynamic). This model computes the driving strategy and control algorithms to control steering, breaking and the powertrain. Additional ADAS functions such as Automated Emergency Braking (AEB), lane assistance and surround are also deployed on such a platform.

In addition, modern automotive connected systems of systems must guarantee dependable functionality for the high-performance cyber-physical systems. Such requirements carry a potentially conflicting undertone in a sense that the development drivers are pushing for the extremely powerful performance, while the dependability aspect is creating a limiting wrapper around this solution-seeking computational system. That is evident in the available systems on chip, which are predominantly either highly specialized and offer high computing performance (e.g., with multi-core, multi CPUs on a single chip, GPUs), or highly focused on compliance with the relevant safety standards (e.g., Lockstep CPU cores with clock delay, safety management unit, clock and voltage monitors). In order to offer both high-performance and safety features to applications, there is a necessity to provide adequate platform solutions. An essential property of such a platform is called the mixed-criticality. Mixed-criticality systems can execute applications with different criticality levels and provide guarantees that the applications characterised by different criticality levels do not influence each other.

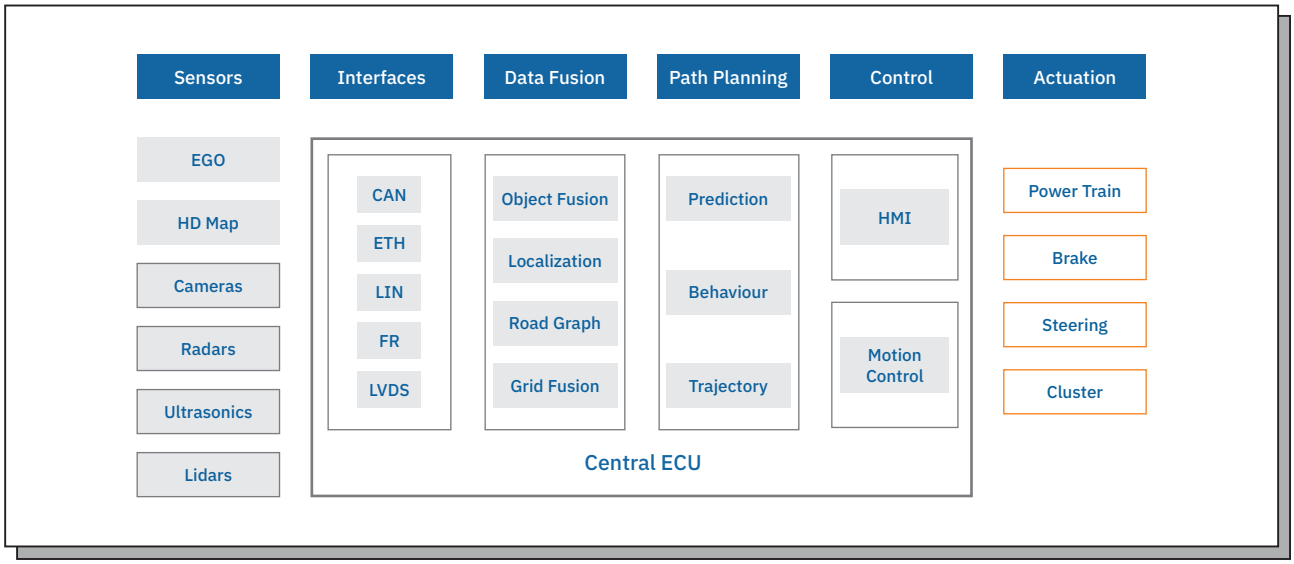

Figure 4: General Automated Driving System Architecture

Section 5.1 describes a demonstration of the development in a rover robot. This demonstration is enabled through the exploitation of the platform's architecture (*Figure 4*), which lends itself to the integration of various automation functionalities.

4.2 Vehicle level

A path towards vehicle demonstration (section 5.2 based on *Figure 5*) integrates new remote-controlled ADAS functionality into an existing serial vehicle Figure 10. The goal is to create a platform for further ADAS and AD prototype applications. The fulfilment of the project requirements goes beyond the vehicle related components and includes newly developed and integrated interface definitions and implementation of control algorithms. In addition, HMI development is implemented on a generic HW platform, which is sporting embedded Linux. Development also targets SW for android devices, secure connection and server-side

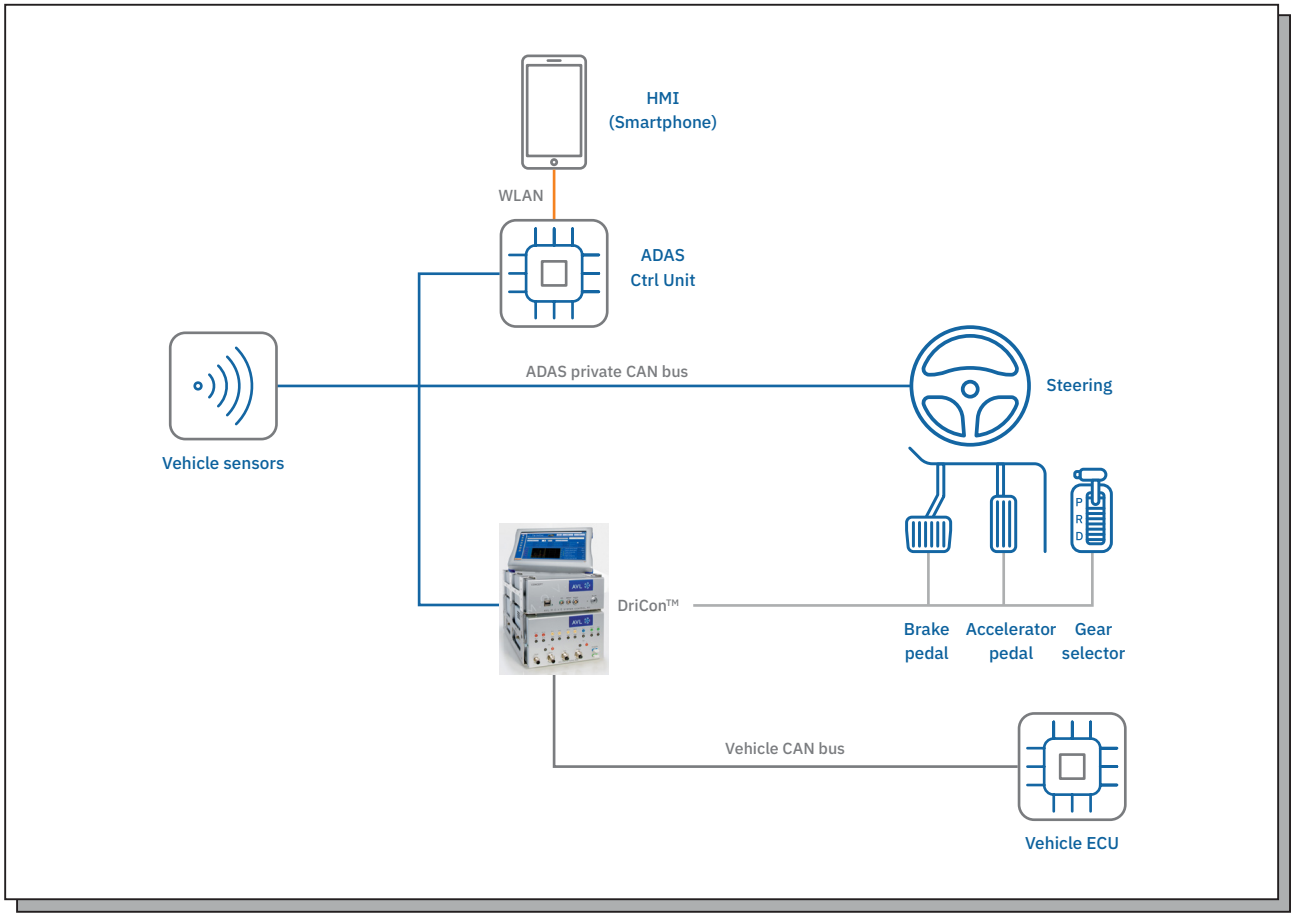

Figure 5: DriConTM as the main gateway between ADAS features or remote HMI input and the vehicle interfaces

software as well as general state-machine that accounts for all possible system states and corresponding behaviour.

AVL's DriConTM interfaces between the ADAS functionality and vehicle controls. DriConTM is a compact driver control tool that offers interaction with vehicle communication channels and control. Its offer of freely definable manoeuvres turns it into a powerful tool for vehicle testing in controlled conditions (e.g. repro-

duction of road measurements). In the context of IoT4CPS, the tool offers a possibility to integrate TTTech's safety platform into a real vehicle and hence, mimic AD in controlled conditions. The resulting capabilities involve the possibility to experiment with and to validate either newly developed AD functionalities or the response of security-relevant technology blocks to the deliberately introduced cyber-security attacks. The tool offers the chance to examine the real response of the vehicle to cyber-attacks and errors on the control signals. Hence, the tool enables interfacing a non-automated vehicle to develop and demonstrate ADAS and AD features and their integration with the security features.

DriConTM enables the control pedals to be subjected to pure electronic control. The vehicle manoeuvres are freely definable in either an event or time-based mode. The safety is guaranteed through the usage of a safety box, which is also capable of providing basic signal conditioning. A Windows-based real-time System Control unit offers computing capabilities for the driving tests. It also enables visualisation (touch screen monitor, or laptop/tablet). The key intended functionality in this setup is to control the vehicle (velocity and direction). Hence, the standard vehicle controls (accelerator, brake, steering and torque) are disconnected from the vehicle's ECU and are replaced with the manipulated DriConTM signals. Although DriConTM offers limited intelligence, in this setup its intended usage is to route control signals from the TTTech Safety Platform to the vehicle's ECU. An assumption is that all the necessary processing is performed in the Safety Platform and DriConTM acts as an actuator controller.

Previous use cases, which helped pave the way for the development of DriConTM include smartphone-controlled remote parking. A firm overlap of that previous use case with this test setup is emerging from the need for a secure application for wireless communication. Such application is strengthening the argument and justification for the tool as many use cases are susceptible to dependability aspects – especially security, which is tightly interlinked in the safety of the road users.

DriConTM is receiving demand information for vehicle functions from the ADAS system and is responsible for interfacing them with the vehicle. AVL DriConTM is interfacing to the accelerator pedal, brake pedal, steering and lever. An additional switch routes the signal flow either via DriConTM (ADAS Mode) or leaves the signal flow in the original state. The connection to the vehicle's CAN bus enables DriConTM to receive vehicle signals, such as vehicle speed, accelerator pedal position, brake pressure, steering angle and lever position. The communication from DriConTM to the ADAS system is via a private CAN bus, allowing communication with the HMI. The user may demand forward and backward driving, as well as steering via the HMI. The DriConTM receives these demands via the private CAN connection. Internal controllers react to these demands and send the appropriate response to the vehicle.

4.3 Security analysis

The vehicle controls setup is analysed from the perspective of potential cyber-security threats using AIT's ThreatGet tool Figure 6, which offers a wide range of components and communication protocols that match the design of several automotive scenarios. The analysis includes vehicle communication to an external unit, which is representable by a road-side unit. It also models a Linux firmware unit within the AD platform

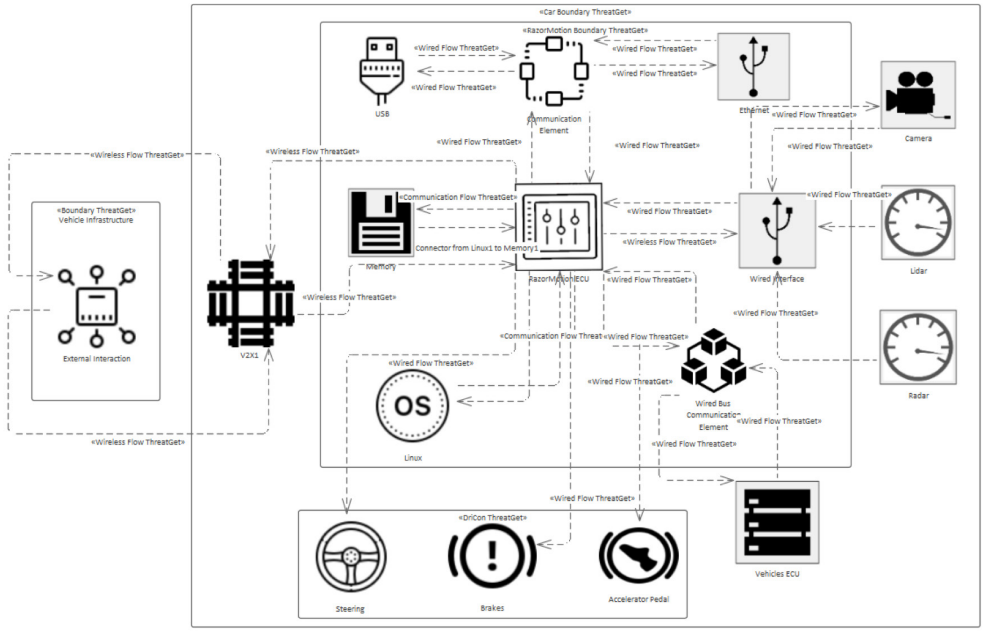

Figure 6: Generalised threat model of the current setup

and defines a set of security measures applied to the new elements.

ThreatGet checks the communication flow between interconnected units to identify possible threats that could affect the vehicular system. As specified in the threat model, the vehicle communicates via the V2X unit with an external interaction unit. A typical potential threat is modelled i.e. a spoofing attack, which is represented as a sequence of malicious actions an adversary performs to impersonate an external infrastructure unit. ThreatGet leverages vehicle boundary concept to examine the integrity of communication flow and the security measures of the external source unit and is able to detect a risk of a spoofing attack. Due to complexity, details are abstracted away to acquire a more general threat model. The purpose of this generalized model is to serve practitioners who intend to specialize it further, depending on the concrete AD platform of interest. It is possible to extend the current threat model beyond the current setup to cover real-scale industrial AD architecture.

Upon the model setup with the intended security measures, the security vulnerabilities are analysed based on domain knowledge in ThreatGet's internal threat database. The identified threats are classified and the following automated evaluation is used to assesses the overall risk to the system. The evaluated assessment is based on impact and likelihood parameter values for each threat. To minimise risks, security measures are activated. These could include authentication, authorisation, access control, encryption and others. The repeated evaluation helps establish the success factor of the recommended security measures and to what extent they help reduce the risks.

5. APPLICATION

Two demonstration steps are created by IoT4CPS. The first one (section 5.1) is represented by a rover robot, which offers initial testing capabilities. The more advanced scenario is demonstrated on a real vehicle (section 5.2), where some of those initial concepts are replicated in real driving scenarios. Both scenarios are built onto the development from section 4.

5.1 Rover robot

A rover robot application scenario is designed and it demonstrates a possibility to develop and test automated driving functions in a safe and controlled environment. It establishes a path towards integration of IoT4CPS technology into a real automotive application of automated driving. For this purpose, the demonstrator based on the mobile rover robot (TUW) was designed (*Figure 7*). The safe and secure platform (TTTech) for highly automated driving was integrated, together with a set of sensors and actuators showing the performance of the design simulating a highly automated driving capable vehicle.
In this case, the collision avoidance and the case of a safety-relevant failure of a lidar sensor are shown. The system contains a smart watchdog to monitor the functionality of components and a self-healing engine. The failure is simulated by powering off the laser scanner. The failure is detected and healed by the SHSA (Self-healing by structural adaptation, see D6.1a), by replacing a failed component with a substitute component. After the failure is detected, a substitute node is generated, and the sonar is used to measure the distance. Sonar is considered as an emergency operation mode (for utilisation in the field, timings for fault detection/transition to sonar operation will be specified). The solution is a further extendable through the addition of other automated driving functionalities for testing. At the hardware level, the current setup lends itself to further expansion for testing of other hardware components (primarily sensors).

The initial demonstration showcases control potential of the safety platform. The control computer controlling the robot hosts an application capable of avoiding collisions in an autonomous manner. The developed architecture is fully deployed and engages several ECUs and sensors (*Figure 8*). The robot carries the TTTech safety Platform, a Raspberry Pi module as computing platforms and a LASER Scanner as well as a

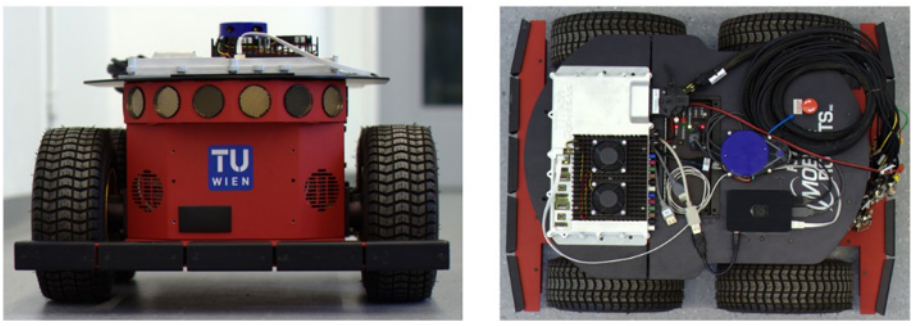

Figure 7: Mobile rover robot equipped (left - front view) sonars and (right - top view) TTTech's safety platform, a Raspberry Pi and the LIDAR measuring the distance to obstacles

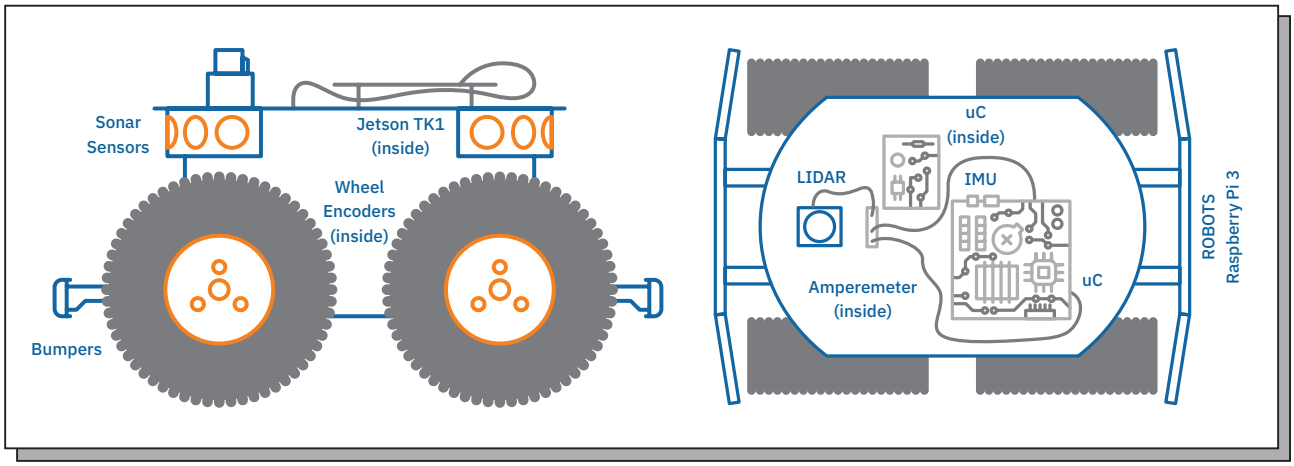

Figure 8: Mobile robot equipped with its sensors and processing units

LIDAR to measure distances to potential objects. The main showcased functionality of the presented CPS is that of a "collision avoidance system".

The platform's hardware architecture consists of different computing modules: a safety microcontroller and two high-performance CPUs based on ARM architecture. These devices are connected by a Deterministic Ethernet (DE) switch. External interfaces such as CAN or Ethernet are also provided. The platform's external interfaces are grouped into: (1) Vehicle connector (power feed, communication busses, IOs), (2) Video input connectors (camera inputs), (3) Video output connectors (display outputs for dashboard and infotainment) and (4) Programming and debugging interfaces connectors (internal, accessible via a hatch in the housing). Both platforms run Linux and the Robot Operating System ROS as middleware connecting different software components (ROS nodes). Nodes communicate via a message-based interface over TCP/IP. In particular, ROS nodes subscribe and publish to ROS topics. ROS can start new nodes and reconfigure the communication flow of existing nodes during runtime. For example, there are nodes for lidar data, calculation of the minimal distance or a watchdog.

The application nodes are distributed across two hosts where more critical tasks are planned to run the safety platform. *Figure 9* shows the different hosts and the distribution where components or nodes represent drivers to the sensors and actuators, as well as controllers. For instance, the node emergency_stop is a "critical" ROS node subscribing and publishing topics and it runs on the safety platform. The motors of the rover are controlled by a microcontroller Robot uC. The Pi connects to the microcontroller and LIDAR via UART. A controller running on a computer sends the desired linear and angular velocity (v,ω) to the robot's microcontroller (Robot uC) controlling the wheel motors. The LIDAR (or laser scanner) on top of the rover provides distance measurements of 360°. When the minimum distance in front of the rover (dmin) – calculated by another ROS node (dmin_calculator) falls below a threshold, the mobile rover robot is stopped and the velocity commands from the controller are replaced by (0,0), which is implemented by the node emergency_stop. Acceptance of the controller commands is resumed when dmin again exceeds the threshold.

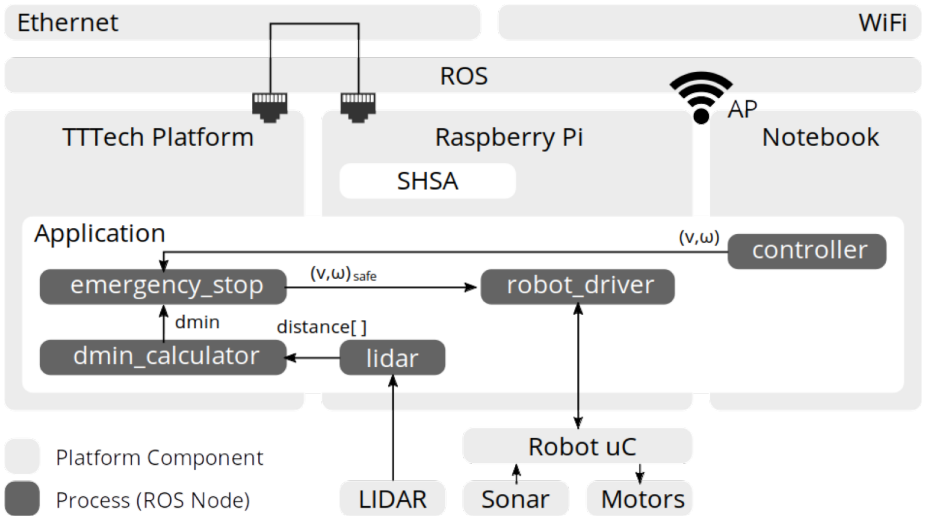

Figure 9: Platform overview and nodes of the application

5.2 Vehicle demonstration

Remote control of the demonstrator vehicle (*Figure 10*) enables safe testing of new functionalities at the real vehicle through enabled access to vehicle interfaces and integration of connectivity solutions. Consequently, the existing setup lends itself to full expansion in terms of sensors, actuators and control modules. Such a testing setup enables benchmarking various options at the early stages of development. It also lends itself to improvements and testing of new HMI solutions. The versatility of testing solutions is possible due to the current generic implementation using an embedded Linux environment. The offered connection to the outside world, which is based on connection to android devices, also leaves a relatively open field in terms of human control. The benefits brought by the development within IoT4CPS have also contributed to the security improvements of the offered test solution. Through the integration of trustworthy IoT methods, which are resulting from IoT4CPS technology development activities, the demonstration also aids the evaluation of communication to remote cloud locations.

The offered solution opens the door to further development of basic IoT solutions and improvement of their security features. These are crucial for the continual development of AD functionality, which is a key component of the ongoing automotive revolution.

Figure 10: Implementing automation functionality at the vehicle level

REFERENCES

[Affenzeller et al, 2016] Affenzeller, J, et al. „Austrian Research, Development & Innovation Roadmap for Automated Vehicles“, BMVIT, 2016.

[Alam, 2010] Alam, A.A., Gattami, A. and Johansson, K. H., „An experimental study on the fuel reduction potential of heavy duty vehicle platooning,“ in Intelligent Transportation Systems (ITSC), 2010 13th International IEEE Conference on , vol., no., pp.306-311, 19-22 Sept. 2010, doi: 10.1109/ITSC.2010.5625054

[Bergenhem, 2012] Bergenhem, Carl, et al. „Overview of platooning systems.“ Proceedings of the 19th ITS World Congress, Oct 22-26, Vienna, Austria (2012). 2012.

[Berger, 2016] Berger, Roland http://www.rolandberger.de/expertise/branchenexpertise/automotive/autonomous-driving.html abgerufen 3.2.2016

[Eichberger, 2011] Eichberger, Arno. “Contributions to primary, secondary and integrated traffic safety”, Verlag Holzhausen, 2011.

[Reddy 2006] Reddy, R., „Robotics and Intelligent Systems in Support of Society,“ in Intelligent Systems, IEEE, vol.21, no.3, pp.24-31, Jan.-Feb. 2006, doi: 10.1109/MIS.2006.57.

[Schramm, 2013] Schramm, Dieter, et al. „Das Automobil im Jahr 2025“. Springer-Verlag. 2013.

[CCR 2016] Connected car report 2016: Opportunities, risk, and turmoil on the road to autonomous vehicles, PWC, https://www.strategyand.pwc.com/reports/connected-car-2016-study

[Andy Greenberg, 2015] video on youtube, Andy Greenberg (Senior Writer, Wired) Charlie Miller (Security Engineer, Cruise Automation) & Chris Valasek (Director Vehicle Safety Research, IQActive) https://www.youtube.com/watch?v=MK0SrxBC1xs

For more information on this document or the IoT4CPS project, please contact:
Mario Drobics, AIT Austrian Institute of Technology, mario.drobics@ait.ac.at

Layout & Grafik

Nora Novak, goldmaedchen Grafikdesign

Legal Notices

The IoT4CPS project is partially funded by the „ICT of the Future“ Program of the FFG and the BMVIT.