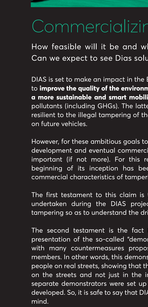
DIAS
DIAGNOSTIC ANTI-TAMPERING SYSTEMS
#2
NEWSLETTER

EDITORIAL



Commercializing Dias solutions

How feasible will it be and what are the plans for doing that? Can we expect to see Dias solutions on vehicles in the future?

DIAS is set to *make an impact* in the European Green Deal. In detail, DIAS aims to **improve the quality of the environment and accelerate the transition towards a more sustainable and smart mobility** by reducing the emissions of harmful pollutants (including GHGs). The latter will be achieved by making the vehicle resilient to the illegal tampering of the environmental protection systems fitted on future vehicles.

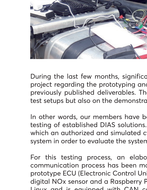
However, for these ambitious goals to be achieved, research is not enough. The development and eventual commercialization of the developed solutions is as important (if not more). For this reason, the DIAS project since the very beginning of its inception has been roving around the market and the commercial characteristics of tampering and antitampering.

The first testament to this claim is the fact that one of the very first tasks undertaken during the DIAS project was to analyze the market around tampering so as to understand the driving force behind this phenomenon.

The second testament is the fact that the last milestone of DIAS is the presentation of the so-called "demonstrator vehicle", which will be equipped with many countermeasures proposed and developed by the consortium members. In other words, this demonstrator will be a real vehicle, driven by real people on real streets, showing that the solutions proposed by DIAS also belong on the streets and not just in the imagination of its engineers. In addition, separate demonstrators were set up for a few standalone features that were developed. So, it is safe to say that DIAS both starts and ends with the market in mind.

But the ways DIAS is involved with the tampering and antitampering market do not end there. During the whole countermeasure development phase, our engineers tried to make use of well-established and known technologies (such as CAN bus) as the underlying foundation for the solutions developed. Also, our members not only have excellent field knowledge of the automotive industry, but they have also been in very close contact with other industrial partners in order to find the best possible compromise between what is desirable and what is feasible. Summing up: the industry will not have to re-invent the wheel, many solutions can be rapidly deployed and consumers won't have to pay a heavy bill for it.

The story so far



During the last few months, significant progress has been made in the DIAS project regarding the prototyping and testing of the solutions described in the previously published deliverables. The tests were performed both on desktop test setups but also on the demonstrator vehicle.

In other words, our members have been tirelessly working on the penetration testing of established DIAS solutions. Penetration testing is the test process in which an authorized and simulated cyber attack is performed on a computing system in order to evaluate the system's security and resilience.

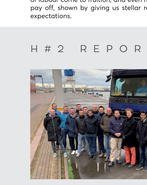
For this testing process, an elaborate setup that aims to simulate the communication process has been manufactured. The setup is comprised of a prototype ECU (Electronic Control Unit) that runs all the latest DIAS solutions, a digital NOx sensor and a Raspberry Pi single board computer that runs on Kali Linux and is equipped with CAN controllers, so it can have access to the communication channel between the ECU and the digital NOx sensor. All the components are connected with a custom-made harness.

As regards the communication channel between the ECU and the digital NOx sensor, the "SecOC light" has been developed with consideration for the computational restrictions of the digital sensors.

As far as the ECU is concerned, it contains the latest developments concerning the diagnostic system proposed by DIAS along with security techniques aimed at reducing the attack surface, such as secure boot, secure software updating and code signing.

All the members in the DIAS consortium are thrilled to start seeing a major piece of labour come to fruition, and even more thrilled to see that the hard work did pay off, shown by giving us stellar results that have exceeded even our own expectations.

H#2 REPORT

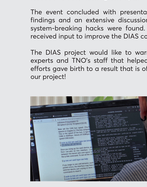


The "Hack-A-Truck Part 2" Hackathon was successfully held in March 2022 in Rotterdam, Netherlands. The former yard of the Rotterdamsche Droogdok Maatschappij (RDM), right in the middle of the port and it proved to be the perfect place for such an event.

The target was to evaluate the new features for tampering prevention and detection that have been added since the first hacking event (May 2021). Hack-a-Truck Part 2 revolved around a new system that wirelessly reports information about a possible tampering suspicion to a cloud or a supervising entity, to enable fast and easy detection and repair tampering in connected vehicles. Participants had to do their best against the cutting-edge technologies implemented in the DIAS countermeasures.

The event was divided into two parts: an online preparatory session and a 2-day hybrid event. In the first session, the 15 external independent participants, ranging from students to professional ethical hackers, with expertise in automotive communication and security, got up to speed with training sessions on the latest environmental protection systems and the newly developed state-of-the-art countermeasures.

During the 2-day hybrid (physical and in-person) event, the participants worked on 2 testbeds that were prepared by DIAS partners: one on the in-vehicle communication of control units and one on the wireless communication between the in-vehicle control units and the cloud.



A pool of DIAS experts from - amongst others - Bosch, FEV, UMFST and CERTH/ITI were present during the event to answer questions and provide early feedback on the hacking attempts.

The event concluded with presentations from the participants about their findings and an extensive discussion with DIAS experts. At first glance, no system-breaking hacks were found. DIAS experts are further analyzing the received input to improve the DIAS countermeasures.

The DIAS project would like to warmly thank all the participants, mentors, experts and TNO's staff that helped this hackathon become a reality! Your efforts gave birth to a result that is of paramount importance to the fruition of our project!

Meet the partners

The Laboratory of Applied Thermodynamics was founded in 1974, as part of the Faculty of Engineering, at the Aristotle University of Thessaloniki its educational and research activities cover the following fields: Applied thermodynamics and combustion, internal combustion engines and missions control, emissions inventories and forecasts and energy policy and renewable energy sources. LAT is coordinating the DIAS project and in parallel, is responsible for the development of the legislative anti-tampering requirements. Finally, LAT contributed to the market analysis and assessment of tampering systems.

The Netherlands Organisation for Applied Scientific Research (TNO) is an independent research organisation. We connect people and knowledge to create innovations that boost the sustainable competitive strength of industry and the well-being of society now and in the future. Together with our partners, we focus on the societal challenges of a safe, healthy, sustainable and digital society. This is our mission and it is what drives us, the over 3600 professionals at TNO, in our work every day. As far as DIAS is concerned, TNO is the leader of Work Package 3 which involves the market analysis and assessment of tampering systems.

INTERNET SEARCH CHALLENGE

How safe do you think your vehicle really is from a tampering perspective? Try searching for "ECU tampering" in your preferred search engine. Maybe even try the search followed by the make and model of your vehicle, to see what other people have managed to accomplish. The chances are that someone has already managed to gain access to the type of ECU on your vehicle. Despite having made our cars faster, more efficient, safer and more comfortable, when ECUs were initially designed, security was not the first priority. In the DIAS project, our goal is to ensure that any component - including the ECU - that belongs to the environmental protection system of a vehicle can be accessed and modified only for legitimate purposes.

STAY TUNED

The *Final Dissemination Event* of the DIAS project will take place on **Tuesday 25th of October, 2022**. Click here for more details.

DIAS
Call: H2020-MG-2018-TwoStages

The DIAS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 814951